TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

TUOMAS NUMMI

ERP-VERKKOPALVELUN TUOTANNON RISKINHALLINTA

Diplomityö

Tarkastaja: professori Kari Systä
Tarkastaja ja aihe hyväksytty
Tieto- ja sähkötekniikan
tiedekuntaneuvoston kokouksessa
13. elokuuta 2014

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Tietotekniikan koulutusohjelma
NUMMI, TUOMAS: ERP-verkkopalvelun tuotannon riskinhallinta
Diplomityö, 54 sivua, 7 liitesivua
Lokakuu 2014
Pääaine: Ohjelmistotuotanto
Tarkastaja: professori Kari Systä
Avainsanat: Riskinhallinta, projekti, ohjelmisto, verkkopalvelu, ERP

Diplomityön tavoitteena on ollut kehittää riskinhallintamenetelmä, jonka Agenteq Solutions Oy -niminen yritys voi ottaa osaksi tuotantoprosessejaan. Tavoitteena oli löytää käyttöönottokynnykseltään matala menetelmä yritykselle, jolla ei ole aikaisemmin ollut käytössä varsinaista riskinhallintamenetelmää.

Riskinhallintaprosessi jakautuu teoriassa neljään vaiheeseen: riskien tunnistaminen, riskianalyysi, riskisuunnittelu ja riskien valvonta. Tunnistamisvaiheessa etsitään ja listataan olemassa olevat riskit. Riskianalyysissä käydään riskit läpi, määrittäen niiden vaikutukset ja todennäköisyydet. Samalla muodostuu riskien keskinäinen priorisointi. Riskisuunnittelussa selvitetään kaikille riskeille välttämis- tai lievennystoimenpiteet, joiden avulla riskien vaikutukset saadaan hyväksyttävälle tasolle. Riskien valvonta tarkoittaa, että tarkkaillaan tilannetta riskinhallinnan kohteena olevassa toiminnassa. Valvonnassa puututaan mahdollisiin uusiin tai muuttuviin tunnettuihin riskeihin.

Riskinhallinnan teorian soveltamiseksi tarvitaan käytännön menetelmä. Tässä työssä on sovellettu OCTAVE Allegro –riskinhallintamenetelmää. OCTAVE Allegro -menetelmä käy läpi samat vaiheet kuin teoriaosuudessa on esitetty, mutta uhkasuuntautuneena menetelmänä sen lähtökohtana ovat olleet erilaisiin resursseihin kohdistuvat uhat. Riskit on selvitetty kartoittamalla yrityksen kannalta tärkeät resurssit. Lisäksi selvitetään niihin kohdistuvat uhat sekä uhkien potentiaaliset vaikutukset. Uhista ja niiden vaikutuksista on muodostettu riskilistat, joita on käsitelty teoriaosuudessa esitettyjen vaiheiden mukaisesti.

Tuloksena syntynyt menetelmä tarjoaa helpon lähestymistavan riskinhallintaan. Se voidaan ottaa käyttöön portaittain ensin vain tietyissä Agenteqin prosesseissa, jolloin saadaan vähitellen lisättyä riskinhallintatietämystä organisaation sisällä. Varsinkin alkuvaiheessa suurimpana haasteena on riskinhallinnan vaatima panostus. Tuotantoprosessien toiminta on hajautunut monelle eri taholle, jolloin kattavaan riskinhallintaan tarvitaan henkilöstöä jokaisesta eri vaiheesta tuotantoprosessia. Resurssivaatimusten takia yrityksen johto onkin avainasemassa riskinhallinnan käyttöönotossa ja riskinhallintastrategian suunnittelussa.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Programme in Information Technology
NUMMI, TUOMAS: Risk Management in an ERP online service production
Master of Science Thesis, 54 pages, 7 Appendix pages
October 2014
Major: Software Engineering
Examiner: Professor Kari Systä
Keywords: Risk management, project, software, online service, ERP

The objective of this thesis has been to create a risk management method for Agenteq Solutions Ltd. to use in their processes. The goal was to find a method which is easy to apply in practice, as there is no previous experience of risk management methods in the company.

Risk management process is divided into four phases: risk identification, risk analysis, risk planning and risk monitoring. In the identification phase, the risks are searched for and listed. Risk analysis consists of determining the effects and probabilities for each individual risk, thus creating priorities for them. In risk planning, each risk is assessed and avoidance and migitation strategies are created for them to reduce the risks to an acceptable level. Risk monitoring means actions to observe changes in the target process, and if necessary, taking into account changes in the existing risks and also new risks that emerge.

In addition to the risk management theory, a practical method is needed. In this thesis, OCTAVE Allegro risk management method was used as a base, and it was adapted to be used in Agenteq. The method goes through the phases described in the theory section, but as it is a threat oriented method, it derives the risks from threats targeting important resources. Risks are identified by mapping out these threats and their effects. This process results a list of risks, and the list is processed with phases similar to the ones in theory section.

The risk management method that this thesis produced offers an easy approach to risk management. It can be taken into use gradually, one production process at the time. This way, the risk management knowledge inside the company can be increased in a controlled way. The biggest challenge is the need for resources, especially in the early stages of implementing risk management. The processes consists of the effort of multiple parties, and because of that, to make a thorough risk assessment, personnel from each stage of the process must participate. Because of the big demand for resources, the management of the company is the key figure in taking risk management into use.

ALKUSANAT

Tämä diplomityö on osasuoritus diplomi-insinööritutkintoani Tampereen teknillisessä yliopistossa. Työn tarkastaja toimi professori Kari Systä.

Haluan kiittää työnantajaani Agenteq Solutions Oy:tä mahdollisuudesta tehdä diplomityöni aiheesta, joka on oleellisessa osassa jokapäiväisessä työssäni. Ennen kaikkea haluan kiittää läheisiäni, perhettäni ja ystäviäni tuesta ja kannustuksesta opintojeni aikana.

Helsingissä 14.10.2014

Tuomas Nummi

SISÄLLYS

TERMIT JA NIIDEN MÄÄRITELMÄT

ERP	Enterprise resource planning. Toiminnanohjausjärjestelmä.
Product owner	Hallinnoi tiimin tekemiä tehtäviä (ScrumGuides 2014)
Projentinhallintakolmio	Projektinhallinan apuväline, joka kuvastaa projektin osa-alueiden suhdetta toisiinsa (McGhee & McAliney 2007, s. 74)
Riskinhallintaorganisaatio	Ryhmä yrituksen henkilöstöä, joka on vastuussa riskinhallinnan täytäntöönpanosta (Protiviti 2013)
Tampuuri	Toiminnanohjaus- ja asiakkuudenhoitojärjestelmä, verkkopalvelu kiinteistötiedon hallintaan.
Scrum	Projektinhallinnan viitekehys (ScrumGuides 2014)
Scrum master	Vastuussa siitä, että tiimi toimii scrumin mukaisesti (ScrumGuides 2014)
Sprint	Scrumin peruskäsite, ajanjakso, jonka aikana tehdään tietyt tehtävät (ScrumGuides 2014)
Sprint planning	Tapahtuma, jossa scrum-tiimi suunnittelee tulevan sprintin tehtävät (ScrumGuides 2014)
SWOT-analyysi	Analysointimenetelmä vahvuuksien, heikkouksien, mahdollisuuksien ja uhkien selvittämiseen (Suomen Riskinhallintayhdistys 2014)

1 JOHDANTO

Tämän diplomityön tarkoitus on kartoittaa ohjelmistoprojektin riskinhallintamenetelmiä, ja niiden perusteella kehittää sopiva riskinhallintamalli Agenteq Solutions Oy:n käyttöön. Agenteqilla ei ole käytössä varsinaista riskinhallintamenetelmää, ja tästä syystä sellaista nyt kehitetään. Työssä selvitetään, miten ja millaisia projekteja Agenteqissa käydään läpi. Varsinaisen projektin riskinhallinnan lisäksi, käsitellään myös yrityksen toimintaan liittyviä prosesseja, jotka luonteeltaan vastaavat projekteja.

Työssä esitellään projektin riskinhallinnan teoriaa, ja sen pohjalta käydään läpi Agenteqin käytäntöjä, ja mitä haasteita ne riskinhallinnan suunnittelulle asettavat. Riskienhallinnan teorian ja Agenteqin prosessien käsittelyn jälkeen on tiedossa pääpiirteittäin kuva Agenteqin toiminnasta ja merkittävimmistä riskinhallinnan haasteista. Tämän jälkeen voidaan kehittää yritykselle riskinhallintasuunnitelma, joka valmistuttuaan palvelee Agenteqin eri prosessien riskinhallintaa. Riskinhallintamallissa otetaan huomioon Agenteqin ohjelmistokehitysmalli. Työssä hyödynnetään valmista OCTAVE Allegro -riskinhallintamenetelmää soveltuvin osin. Kyseinen menetelmä valittu, koska sitä on yrityksessä jo aikaisemmin käytetty tietoturvariskien kartoittamiseen, ja se soveltuu hyvin yrityksen riskinhallintalähtökohtiin.

Varsinaisen riskinhallintamenetelmän lisäksi käsitellään Agenteqin näkökulmasta riskinhallintaprosessin oleellista osaa, riskinhallintaorganisaatiota. Riskinhallintaorganisaation tulee koostua sellaisista henkilöstön jäsenistä, että riskinhallinnan kaikki osa-alueet saadaan otettua huomioon riittävän hyvin. Käytännössä lopputuloksena tulisi olla tapa määrittää projektinhallintaorganisaatio aina uuden prosessin alkaessa, sisältäen henkilöstöä tuotehallinnasta ja tuotannosta, riskinhallintapäälliköstä lähtien.

Tavoitteena on luoda suunnitelma, joita noudattamalla saadaan Agenteqissa prosessien osalta käynnistettyä kattava ja luotettava riskinhallinta, ja ylläpidettyä sitä yllä yrityksen toiminnassa. Varsinaisten ohjelmistoprojektien riskinhallinnan lisäksi venytetään riskinhallinta kattamaan muutkin Agenteqin prosessit, jolloin riskinhallinta saadaan ulottumaan jo myyntivaiheeseen asti. Kun työssä esitetty riskinhallintamenetelmä saadaan ajettua sisään yritykseen, saadaan pienennettyä riskien realisoitumisen aiheuttamaa tehokkuuden huonontumista.

2 PROJEKTIT JA RISKINHALLINTA

2.1 Projektit

Niin ohjelmistoalalla kuin muuallakin, projekti on keino saada tietty kokonaisuus hallitusti tehtyä valmiiksi. Ohjelmistoalalla tämä on luonnollista, koska usein kyseessä on tietty asia tai kokonaisuus, joka on tavoitteena saada tulokseksi projektin päättyessä. Käytännössä projekti koostuu usein osaprojekteista kuten määrittely- ja toteutusprojekteista. Tämä johtuu esimerkiksi siitä, että projektin alussa määrittelyvaiheessa voidaan hyvinkin tulla siihen tulokseen, että hanke keskeytetään. Ohjelmistoprojekteissa osaprojekteja voivat olla määrittelyn ja toteutuksen lisäksi esimerkiksi käyttöönotto- ja koulutusprojektit. (Haikala & Märijärvi 2004, s. 53)

Projektin laajuus ja rakenne voi riippua merkittävästi siitä, millaista tapausta käsitellään. Tässä diplomityössä käsitellään sellaisia projekteja ja prosesseja, joissa yritys itse tuottaa tuotteen tai palvelun asiakkaalle, ja projektin kaikki vaiheet asiakkaalle toimitukseen asti toteutetaan yrityksen omilla resursseilla. Asiakkaalle myyty tuote ei tässä tapauksessa ole aina sama, vaan vaihtelee asiakaskohtaisesti. Asiakaskohtaisessa räätälöinnissä tuotteenhallinnalla on erittäin keskeinen merkitys. (Haikala & Märijärvi 2004, s. 54)

2.2 Riskinhallinta

Riskin voidaan ymmärtää tarkoittavan eri asioita ympäristöstä ja toimialasta riippuen. Kuitenkin yhteistä näille on epävarmuus, epäonnistuminen ja vastoinkäymiset. Jos riski ja riskinhallinta ovat käsitteenä esimerkiksi yrityksen sisällä epäselviä, seuraa siitä ongelmia. (McManus 2004, s. 3)

Riskinhallinnan merkitys projektipäällikön tehtävissä kasvaa koko ajan. Tämä tarkoittaa sitä, että on valvottava projektin aikatauluun ja tuotettavan ohjelmiston laatuun vaikuttavien riskien ilmenemistä. Jos realisoituvia riskejä havaitaan, on ryhdyttävä toimeen. Riskinhallintaa voidaan parantaa tekemällä projektin alussa riskianalyysi, jossa luetellaan mahdolliset projektiin kohdistuvat riskit, niiden todennäköisyys ja vaikutukset. Kun riskeihin voidaan puuttua nopeammin ja tehokkaammin, eivät taloudelliset ja aikataululliset ongelmat pääse realisoitumaan niin pahasti. (Sommerville 2007, s. 104)

Kun riskienhallintaa otetaan käyttöön, saattaa se näyttää vain lisäävän kompleksisuutta jo valmiiksi kompleksisiin hankkeisiin. Ongelman ehkäiseminen on kuitenkin parempaa

kuin sen hoitaminen. (McManus 2004 s. 4) McManus (2004 s. 4) luettelee syitä, miksi riskinhallintatoiminnot tekevätkin ohjelmistoprojekteista vähemmän monimutkaisia. Riskien tunnistaminen ja priorisointi mahdollistavat projektihenkilöstön keskittymisen projektin oleellisempiin osiin. Riskien lievennystoimenpiteet vähentävät projektin kokonaisriskiä ja täten nopeuttavat projektin valmistumista. Riskinhallinnan avulla nopeammin valmistuvat projektit maksavat vähemmän, ja lisäksi lievennysmenetelmät edelleen vähentävät projektin kuluja. Riskinhallinnan avulla projektien aikataulut voidaan ennustaa paremmin. Yllätysten todennäköisyys on pienempi, koska riskeihin voidaan varautua ja siten reagoida ennen kuin niistä tulee varsinaisia ongelmia. Näitä kaikkia neljää asiaa yhdistää loppujen lopuksi se, että resurssit ovat tehokkaammin käytössä, aikatauluja voidaan ennustaa ja asiakastyytyväisyys kasvaa. Nämä kaikki taas vaikuttavat positiivisesti yrityksen tulokseen.

2.3 Riskinhallintastrategian kehittäminen

Riskienhallinnan varsinainen arvo tulee siitä, että sen avulla saadaan säästettyä projektien tuotantokustannuksissa. Riskienhallinnan käyttöönotto yrityksen projekteissa kuitenkin tarvitsee myös panostusta. (McManus 2004, s. 14) McManus (2004, s. 14) käy läpi riskinhallintastrategian pääpisteitä. Niitä ovat riskinhallinnan sulauttaminen osaksi yrityksen normaalia toimintatapaa sekä tietämyksen lisääminen ja tiedon jakaminen yrityksessä. Myös riskinhallinnan vastuiden ja rakenteen parantaminen ja vakiintuneen termistön luominen riskinhallinnalle ovat tärkeässä osassa. Standardimaisen terminologian ja riskinhallinnan noudattaminen on myös McManusin mukaan peruselementti riskinhallinnassa. Näihin riskinhallinnan tavoitteisiin yhdistyy esimerkiksi seuraavia päämääriä: yrityksen toimenkuvan mukaisten tulosten tuottaminen jatkossakin, yrityksen maineen parantaminen sidosryhmissä, yrityksen edun ja tavoitteiden suojeleminen, henkilöstön tavoitteiden suojeleminen sekä riskienhallintamenetelmien ja –ajatusten soveltaminen päivittäisessä työssä.

Jotta riskinhallinta saadaan sulautettua osaksi yrityskulttuuria, vaatii se kommunikointia, harjoittelua ja koulutusta. Varmistaakseen tämän toteutumisen, tulee seuraavien asioiden täyttyä yrityksen näkökulmasta (McManus 2004 s. 27):

- Riskinhallintarungon hyväksyminen
- Yrityksen johdon sitoutuminen riskinhallintaan
- Riskien vastatoimien strategian luominen
- Riskinhallintaprosessin valvonta
- Riskinhallintaprosessin muutosten vastuunjako
- Riskikulttuurin vahvistaminen henkilöstön kautta
- Kommunikointi ja koulutus
- Sitoutuminen riittävään resursointiin

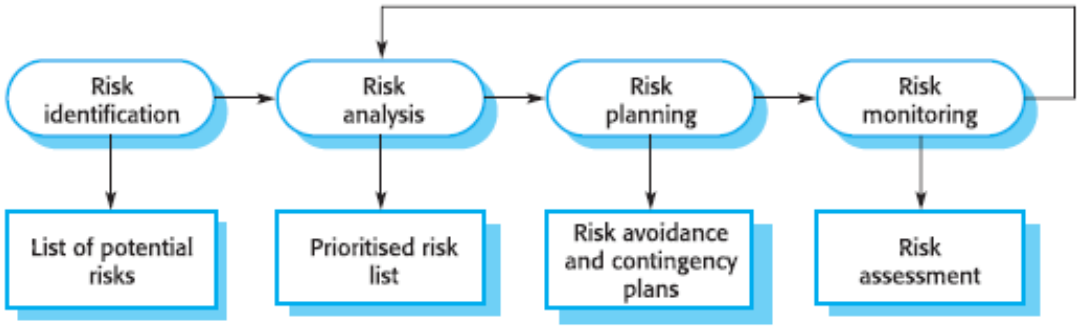
Näiden kohtien täyttyessä yrityksen riskinhallinnan tulisi kehittyä. Lopulta koko riskinhallinnan tavoite on riskien ehkäiseminen, lieventäminen ja korjaaminen, ja sitä kautta taloudellisten tappioiden minimointi (McManus 2004 s. 32).

2.4 Riskinhallintaprosessi

Riskinhallintaprosessi voidaan jakaa neljään vaiheeseen (Sommerville 2007, s. 106):

1. Riskin tunnistaminen. Havaitaan olemassa oleva riskitekijä.
2. Riskianalyysi. Arvioidaan ensimmäisessä vaiheessa tunnistettujen riskien toteutumisten todennäköisyydet ja seurausten vakavuus.
3. Riskisuunnittelu. Jokaisen arvioidun riskin kohdalla suunnitellaan toimenpiteet sen toteutumisen varalle.
4. Riskinvalvonta. Riskejä ja niiden ratkaisutoimenpiteitä arvioidaan jatkuvasti, jotta voidaan ottaa huomioon mahdolliset muutokset edellisen kolmen vaiheen osalta yksittäisellä riskillä.

Riskinhallintaprosessia on havainnollistettu kuvassa 2.1. Koska ohjelmistoprojekteissa usein tapahtuu odottamattomia muutoksia (esimerkiksi aikataulun ja resurssien suhteen), kuvaa viimeinen vaihe hyvin koko riskienhallintaprosessia. Prosessi on iteratiivinen, koska projektin tila muuttuu ilman riskien realisoitumistakin koko elinkaaren ajan. Edellä mainitun riskinhallintaprosessin lisäksi on tärkeää muistaa dokumentoida myös riskinhallinnan toimintaa, joko mahdollisiin ongelmakohtiin puuttumiseksi jo kyseisen projektin aikana, tai sitten taustatiedoksi seuraavaa projektia ja sen riskinhallintaprosessia varten.



Kuva 2.1. *Riskinhallintaprosessi (Sommerville 2007 s. 106)*

McManus (2004 s. 63) kuvaa riskinhallintaprosessin kulun pääpiirteissään samanlaiseksi kuin Sommerville. Kuvassa 2.2. hän määrittää lisäksi vastuuhenkilöt ja ajankohdat projektin aikajanalla, joihin vaiheet sijoittuvat. Erona Sommervillen vastaavaan malliin McManus jakaa valvontavaiheen pienempiin osiin.

Stages →					
Identify	**Analyse**	**Plan**	**Track**	**Control**	**Review**
Who: Project manager	Who: Whole project team	Who: Project manager	Who: Project office	Who: Project office	Who: Project manager and other team members
When: Start of project	When: Start of project	When: Start of project	When: As required	When: As required	When: As required

Kuva 2.2. *Riskien vastuumatriisi (McManus 2004, s. 16)*

2.4.1 Riskien arviointi

Riskien arviointi käsitteenä ei vastaa suoraan tiettyjä vaiheita edellä esitellyssä riskinhallintaprosessissa. Riskin arvioinnilla tarkoitetaan tässä enemmänkin yksittäisen riskin elinkaarta, kuin riskinhallintaprosessia. Arviointi on osa kolmea ensimmäistä kuvassa 2.1. esitettyä vaihetta, ja lisäksi ulottuu myös ajalle ennen riskien tunnistamista. McManus (2004 s. 63) kertoo riskien arvioinnin sisällön. Aluksi tulee määrittää projektin lähtökohta, eli mitä projekti tavoittelee ja mikä määrittää sen onnistumisen. Pitää arvioida, mikä tulisi olemaan projektin lopputulos sen nykyisen riskitilanteen vallitessa, ilman uusien riskinhallintamenetelmien käyttöönottoa. Lisäksi tulee hahmottaa selkeä kuva siitä, mitä seurauksia projektin eri osa-alueiden ongelmakohdat voivat aiheuttaa. Myös nykyisen riskinhallinnan laajuus pitää selvittää, ja riskinhallinnan parantamisprosessin mahdolliset ongelmat kartoittaa.

Lisäksi pitää luoda varsinaiset suunnitelmat riskien lieventämiseksi. Pitää luoda strategiat tarvittavien lievennys- ja poistotoimien tekemiseksi havaitulle riskille. Taustalla pitää olla resursseja, joilla voidaan nopeasti vastata ja toimia riskien realisoituessa. Riskien sattuessa pitää myös olla olemassa menetelmät ja keinot korvata riskistä kärsinyt osa projektia. Näiden lisäksi voidaan pitää mielessä, että riskin toteuduttua se voidaan siirtää esimerkiksi toiselle vastuutiimille, joka osaa paremmin toimia jo tapahtuneiden riskien kanssa. (McManus 2004 s. 63 – 64)

Sommerville (2007, s. 104-105) jakaa riskit kolmeen kategoriaan:

1. Projektiriskit ovat riskejä, jotka vaikuttavat aikatauluun tai resursseihin, esimerkiksi tuotantotiimin avainhenkilön menetys.
2. Tuoteriskit ovat riskejä, jotka vaikuttavat kehitettävän ohjelmiston laatuun ja suorituskykyyn. Esimerkkinä mobiililaitteelle tuotettava ohjelmisto onkin niin raskas, etteivät päätelaitteen resurssit riitä ajamaan sitä.
3. Liiketoimintariskit ovat riskejä, jotka liittyvät ohjelmistoa tuottavaan yritykseen, esimerkiksi kilpailijan julkaisema vastaava tuote.

Kategoriat eivät ole tiukkaan rajattuja, vaan jopa mainitut esimerkit voivat hyvin pitää sisällään vaikutuksia, jotka sopivatkin jonkin toisen kategorian määrittelyyn.

McManus (2004 s. 63 – 64) jakaa riskit myös kolmeen kategoriaan. Nämä kuitenkin hieman eroavat Sommervillen vastaavista. Liiketoimintariskit vaikuttavat yleisesti projektin tavoitteiden täyttymiseen. Teknisiä riskejä voi esiintyä pitkin ohjelmiston elinkaaren, ovat kunkin osa-alueen vastuutahon hallinnassa. Ulkoiset riskit voivat tulla esimerkiksi lainsäädännön tai toimialamuutosten kautta.

Näissä kahdessa kategoriajaottelussa kirjoittajat käyttävät kategorioille eri nimityksiä, ja nimitykset ovat jopa ristiriidassa toistensa kanssa. Kuitenkin jo edellä mainituista lyhyistä kuvauksista käy ilmi, että käytännössä kyseessä on toisiaan vastaava jako. Sommervillen liiketoimintariskit-kategoria vastaa käytännössä McManusin ulkoisia riskejä. Sommervillen jaottelussa projektiriskit taas sisältää samat aihealueet kuin McManusin listassa liiketoimintariskit. Jäljelle jäävät Sommervillen tuoteriskit ja McManusin tekniset riskit sisältävät myös keskenään samantapaiset kuvaukset. Samankaltaisuutta on havainnollistettu kuvassa 2.3.

McManus	Ulkoiset riskit	Liiketoimintariskit	Tekniset riskit
Sommerville	Liiketoimintariskit	Projektiriskit	Tuoteriskit
Kuvaus	Ulkoiset tekijät: lainsäädäntö, kilpailijat	Projektinäkökulma: tavoitteet, aikataulu, resurssit	Toteutus: laatu, menetelmät, työkalut

Kuva 2.3. *McManusin ja Sommervillen riskikategorioiden vertailu*

Riskit saadaan analysoitua hahmottamalla riskin vaikutukset toteutuessaan. Analyysin jälkeen riskit voidaan priorisoida tärkeytensä mukaan. Tämän jälkeen jäljelle jää vielä jokaiselle riskille tarpeellisten välttämis- tai lievennystoimenpiteiden suunnittelu. Jotta nämä asiat voidaan tehdä, tulee projektipäälliköllä ja tiimillä olla pääsy riittäviin resursseihin. Riskinhallintaa suunnittelevalla ja toteuttavalla tiimillä pitää olla pääsy riskin kannalta oleellisiin tietoihin. Tämä tarkoittaa sitä, että pitää olla yhteys johtoportaaseen ja tietoa resursseista sekä käytössä olevista työkaluista.

2.4.2 Riskien tunnistaminen ohjelmistoprojekteissa

Riskien tunnistaminen on kuvan 2.1. mukaisesti riskinhallinnan ensimmäinen vaihe. Tunnistamisvaiheessa tarkoituksena on vain listata potentiaaliset riskit, sen enempää niitä analysoimatta. Riskien määrä kasvaa ohjelmistoprojektin monimutkaistuessa. Lisäksi riskit itsessään myös muuttuvat monimutkaisemmiksi. Tämän takia on suuri tarve systemaattiselle keinolle löytää olemassa olevat riskit. (McManus 2004 s. 32 – 33) Riskilähteiden löytämiseen tarvitaan kvalitatiivisia menetelmiä, kuten aivoriihet ja

SWOT-analyysit. SWOT-analyysi on analysointimenetelmä, jossa yksi tai useampi analysoija pyrkii arvioimaan toimintaansa tai toiminnan osaa (tässä tapauksessa riskilähtöisesti). Analyysissä käydään läpi sisäisistä asioista vahvuudet (strengths) ja heikkoudet (weaknesses), sekä ulkoisista asioista mahdollisuudet (opportunities) ja uhat (threats). SWOT-analyysin negatiivisista osuuksista, heikkouksista ja uhista saadaan listattua ongelmakohdat. SWOT-analyysin ja muiden menetelmien seurauksena saadaan lista riskeistä, jotka kukin jollakin tavalla vahingoittaisivat projektin tavoiteltuja tuloksia. Suurimpana ongelmana mahdollisen kattavan riskilistan kokoamisessa on se, että riskejä on olemassa niin laajalta alueelta, että niiden kaikkien ”keksiminen” on vaikeaa. Kokonaisuudessaan riskien etsimismetodien tulisi kuitenkin pitää sisällään projektin kaikkien osien systemaattinen läpikäynti. Näiden metodien tulisi olla myös ennakoivia, eikä keskittyä jo olemassa oleviin havaintoihin. Lisäksi riskien tietolähteiden kirjon tulisi olla mahdollisimman laaja, sisältäen mahdolliset riskitietokannat tai tiedot aiemmissa projekteissa havaituista riskeistä ja SWOT-analyysit. (McManus 2004 s. 33 – 34)

Riskit voidaan Sommervillen (2007, s. 107) mukaan jakaa kuuteen eri tyyppiin:

1. Teknologiariskit, jotka piilevät kehityksessä käytettävissä erilaisissa ohjelmistoissa ja laitteistoissa.
2. Henkilöriskit, jotka kohdistuvat tuotantotiimin henkilöihin.
3. Organisaatioriskit ovat riskejä, jotka johtuvat ohjelmiston tuotantoympäristön ympärillä olevasta organisaatiosta.
4. Työkaluriskit johtuvat tuotannossa käytettävistä työkaluista ja niiden toiminnasta.
5. Vaatimusriskit, jotka johtuvat siitä, että asiakas muuttaa vaatimuksiaan kesken tuotannon. Lisäksi, miten tällaista muutosprosessia hallitaan.
6. Arviointiriskit johtuvat resursseihin ja hallinnollisiin piirteisiin liittyvistä arviointivirheistä.

Nämä riskityypit eivät ole mitenkään ainoa ja oikea jaottelumalli. Jokaisen yrityksen ja jokaisen projektin osalta tilanne voi olla niin erilainen, että kaikki edellä mainitut riskityypit eivät esimerkiksi ole mitenkään oleellisia. Yrityksestä riippuen tietyntyyppiset riskit voivat sopia paremmin jonkin muun tyypin alle. Kohdan 2.4 alussa luetellut riskikategoriat ja tässä kohdassa mainitut riskityypit eivät ole toisensa poissulkevia jaotteluita, vaan kategoriat jakavat riskejä enemmänkin liiketoiminnallisten vaikutustensa perusteella, riskityyppien perustuessa riskilähteisiin. Yhdessä nämä tarjoavat monimutkaisilta vaikuttavia mahdollisia riskijaottelukeinoja. Jaon tarkoitus on kuitenkin vain helpottaa ja suoraviivaistaa ongelmien ratkaisemista. Riippuu pitkälti yrityksen toimintatavasta, organisaatiosta ja valinnoista, miten riskejä halutaan jaotella. Oleellista on ottaa huomioon se, että jokainen henkilöstön jäsen tuntee oman työtehtävänsä osa-alueen hyvin, kun taas muiden vastaavista hän ei välttämättä tiedä mitään. Osittain jako siis kannattaa perustaa niin sanotusti vastuualueittain. Toinen peruste jaotteluun on se, että samantyyppisiä ongelmia voidaan usein ratkoa samankaltaisilla menetelmillä. Jos

riskit jaotellaan saman tyypin perusteella samaan ryhmään, ei ole varaa että tuhlattaisiin resursseja saman ongelman ratkaisemiseksi useammassa paikassa samaan aikaan.

Luvussa 4 käsitellään tarkemmin konkreettisia jaotteluita, painotuksia ja osa-alueita riskinhallintaprosessissa. Näissä käytännön toimissa on oleellisena osana myös kohdissa 2.4.1 ja 2.4.2 esitetyt riskikategoria- ja tyyppivaihtoehdot. Kun yrityksessä mietitään käytettäviä riskikategorioita ja -tyyppejä, helpottaa näiden jaotteluiden periaatteellisen eron hahmottaminen. Riskikategoriat jaottelevat riskejä erittäin korkealta tasolta. Ne vaikuttavat enemmänkin yrityksen toiminnan osa-alueiden linjauksiin, eli mitkä asiat yritys kokee tärkeimmiksi ja kriittisimmäksi. Tällä tavalla riskejä saadaan tavallaan priorisoitua jo kategorian valinnan perusteella. Samansuuntaista priorisointia tehdään myöhemmin kohdassa 4.3. Riskityypit taas ovat oleellisia siinä vaiheessa, kun riskit on löydetty ja niitä analysoidaan ja suunnitellaan jatkotoimenpiteitä. Riskityyppien avulla samankaltaiset riskin saadaan niputettua yhteen, jolloin on helpompi hahmottaa tietyn osa-alueen riskien kokonaiskuva, ja mahdollisesti helpottaa lieventämis- ja korjaamiskeinojen suunnittelua. Samantyyppisiä riskejä voidaan lieventää ja korjata samankaltaisilla ratkaisuilla, eikä täten välttämättä ole tarve miettiä jokaisen riskin kohdalla ratkaisua uudelleen alusta asti.

2.4.3 Riskianalyysi

Kuvassa 2.1. kuvatun riskinhallintaprosessin toinen vaihe Sommervillen (2007, s 107 – 108) mukaan on tunnistettujen riskien analysointi. Riskinhallinnan suuri haaste on se, että yrityksen johtoa voi olla vaikea saada ottamaan riskit ja niiden seuraukset tarpeeksi vakavasti. Tämän helpottamiseksi, ja erilaisten riskien keskinäisen vakavuus- ja tärkeysvertailun mahdollistamiseksi tulee käsitellä kolmea asiaa: riskin toteutumisen todennäköisyys, riskin vaikutus ja lopulta näistä kahdesta riippuva riskin lopullinen projektille aiheuttama uhka. Voi käydä myös niin, että jokin korkean todennäköisyyden tai vakavan seurauksen riski jätetään kokonaan huomiotta, koska toinen ominaisuus on arvoltaan niin pieni, ettei siihen riskiin ja sen ehkäisemiseen kannata käyttää resursseja. (McManus 2004 s. 86 – 87)

Riskin todennäköisyyttä voidaan arvioida esimerkiksi viisiportaisella asteikolla, jossa todennäköisyys kasvaa sen mukaan, mitä suurempi arvo on. Riskin todennäköisyys tulee arvioida heti, kun uusi riski löydetään. Tämä riskin löytämisen yhteydessä määritetty todennäköisyys on kuitenkin vain arvio, ja tarvittaessa tätä arvoa on muutettava. Tätä todennäköisyyttä voidaan asteikon 1 - 5 lisäksi kuvata myös portaittain välillä 0,00 – 1,00, ja näitä lukuja sitten käyttää riskien lopullisen vakavuuden laskemiseen. (McManus 2004, s. 87 – 88)

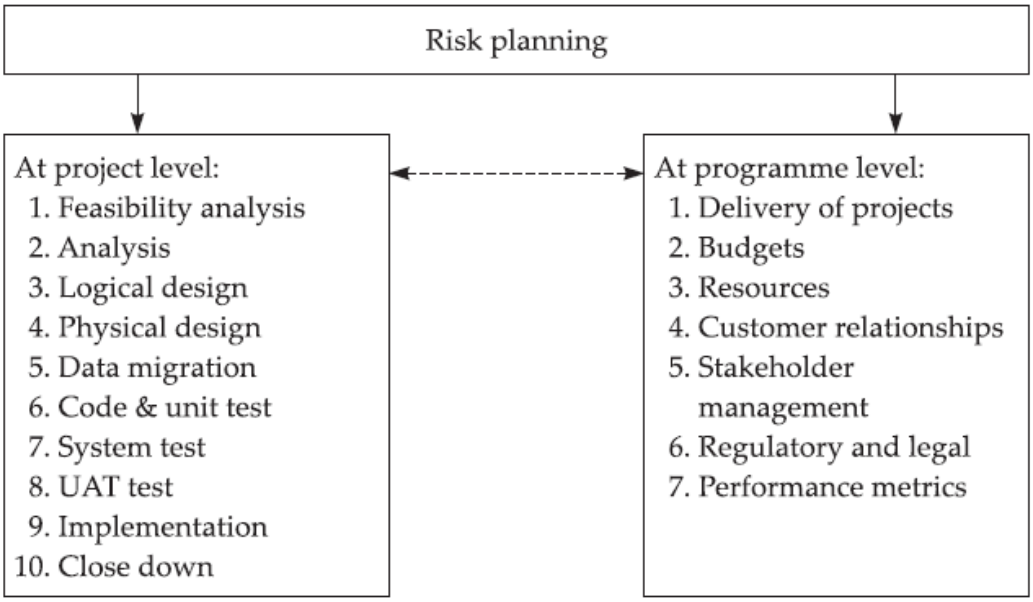
Riskin vaikutusta voidaan niin ikään kuvata viisiportaisella asteikolla. Arviointia voidaan lähestyä esimerkiksi miettimällä paljonko riskin realisoituminen ja siitä palautuminen viivästyttää projektin lopullista valmistumista (ja sitä kautta aiheuttaa taloudellisia menetyksiä). Toinen tapa arviointiin on esimerkiksi suoraan muutoksista ja korjauksista aiheutuvan lisätyön tarve.

Riskin projektille aiheuttama lopullinen uhka voidaan laskea edellisten arvioiden perusteella suoraan kaavalla [todennäköisyys] * [vaikutus]. Näin saadaan edellisiä asteikoita käyttämällä jokaiselle riskille numeerinen arvo väliltä 0 – 25 tai 0,00 – 1,00, riippuen siitä, mitä asteikoita käytetään. Kaikkien riskien arvottaminen tällä kaavalla saattaa tuntua oudolta, koska riskien hahmottaminen ja arviointi saattaa olla tilanteesta riippuen erittäin vaikeaa. Kuitenkin, tällä tavalla saadaan kaikki löydetyt riskit priorisoitua toisiinsa nähden oikeaan prioriteettijärjestykseen. McManus (2004, s. 90) käyttää saatujen numeroarvojen perusteella skaalausta, jossa lopputuloksen perusteella riskin vaikutus luokitellaan asteikolla Matala-Keskiverto-Korkea. McManus painottaa, että koska monesti riskien arviointi on vaikeaa, saattavat aiemmin arvioidut riskit ja niiden ”arvosanat” vääristää myöhemmin arvioitujen riskien jakaumaa. Tämän takia arvioinnissa tulee miettiä minkä tahon mielipiteet kannattaa ottaa eniten huomioon. Jotkut kokevat riskin vaikutukset omassa työssään. Toiset taas ovat ”aiheuttamassa” riskiä tai ovat vastuussa ongelman korjaamisesta. Joidenkin henkilöiden tapauksessa heidän mielipiteensä ja toimintansa itsessään ohjaa muidenkin mielipiteitä.

Tarkoitus ei ole saada aikaan yhdenmukaista mielipidettä, vaan projektipäällikön tulee tuoda selkeästi julki, mikä on riskinhallinnan tavoite ja miksi, jolloin uskalletaan antaa myös eriäviä mielipiteitä. Lisäksi, jos riskien suuruudet arvioi erillinen tiimi, tulee riskit käydä vielä läpi projektipäällikön kanssa ennen kuin ryhdytään suunnittelemaan toimenpiteitä riskien ehkäisemiseksi. Tässä vaiheessa tulee myös käydä läpi, ovatko kaikki havaitut riskit oleellisia projektin kannalta. Tämä tarkoittaa sitä, että onko mitään tehtävissä projektitiimin puolesta. Esimerkiksi toimialalla tapahtuvat muutokset ovat tuotantotiimin ulottumissa, samoin jotkin riskit voivat olla enemmänkin asiakkaan vastuulla. (McManus 2004 s. 90–91)

2.4.4 Riskisuunnittelu

Riskisuunnittelu on erittäin tärkeä osa ohjelmistokehitysprosessia. Varsinkin tuotaessa konkreettista riskinhallintaa uutena asiana organisaatioon, saattaa se vaikuttaa asialta, joka ”tehdään koska on pakko, ja samalla menetetään resursseja tärkeistä asioista”. Riskinhallinta kuitenkin on osa tehokasta johtamista ja työn hallintaa. Riskinhallinta voidaan helposti nähdä taktisena, yksittäisiin ongelmiin ja asioihin puuttumisena, mutta sillä on myös strategisempi puoli, joka mahdollistaa eri osa-alueiden tarkastelun esimerkiksi yrityksen johtotasolla. (McManus 2004, s. 97) Tätä kattavuutta ja monimuotoisuutta kuvaa kuva 2.4.



Kuva 2.4. *Riskisuunnittelu (McManus 2004, s. 97)*

Riskisuunnittelun tavoitteena on saavuttaa optimaalinen tasapaino ja tehokkuus riskinhallinnassa. Tämä tarkoittaa käytännössä sitä, että mitä enemmän riskin lievennyskustannuksissa säästetään, sitä suuremmaksi riskin todennäköisyys ja/tai vaikutus kasvaa. (McManus 2004 s. 97 - 98)

Riskisuunnittelun tavoitteet ovat:

- Määrittää riskien lieventämisen prioriteetit
- Eri vaihtoehtojen löytäminen tehtäviksi toimenpiteiksi
- Varasuunnitelmien määrittäminen
- Päätöstenteko valittavista toimenpiteistä

Käytettävissä tulee olla kaikki riskianalyysissä selvitetyt tiedot riskeistä, jolloin voidaan mahdollisimman tehokkaasti käydä riskikohtaisesti läpi seuraavat vaiheet:

- Riskin aiheellisuus – onko riski enää validi
- Onko kyseessä lyhyen, keskipitkän vai pitkän aikavälin riski
- Riskin määrittelyn tarkkuus nykyisellään
- Todellinen vaikutus projektiin
- Riskin omistus, eli kenen vastuulla riskin valvonta on
- Suunnitelma riskin jatkotoimenpiteiden hyväksymiseksi, lisätutkimus tai toimenpiteet
- Varasuunnitelma riskin realisoitumisen varalle

Tutkimusten mukaan suunnitteluun ja valmisteluun käytettävä aika vaikuttaa suoraan projektin toteutumisen onnistumiseen ja tehokkuuteen. Tähän tavoitteeseen pääsemiseen auttavat tarkkaan määritellyt menettelytavat ja niissä pitäytyminen, jatkuva riskinhallintatoiminnan parantaminen ja pätevä riskinhallintamenetelmiin kouluttautunut

henkilöstö. näiden lisäksi McManus mainitsee myös mittaus- ja riskinhallintatyökalujen käytön. (McManus 2004, s. 99)

2.4.5 Riskien lieventämisstrategiat

Riskien välttämisstrategiat

Riskien välttäminen tarkoittaa käytännössä sitä, että pyritään suunnittelemaan ja määrittämään projektin tavoitteet siten, että minimoidaan riskien realisoitumisen mahdollisuus. Tästä syystä nämä strategiat pitää suunnitella huolella, koska ne saattavat hankaloittaa yritystason tavoitteiden täyttymistä. Tämä suunnittelu kuitenkin vie resursseja. Esimerkiksi jos vältetään tietoturvariskejä, on mahdollista että resurssit (budjetti) loppuvat kesken ennen kuin vakavimmat riskit on saatu estettyä. Käytännössä on olemassa kahdenlaisia varotoimenpiteitä. Uhkavarotoimenpiteet vähentävät uhan mahdollisuutta käyttää haavoittuvuutta hyväkseen (esim. lukot ovissa tai palomuurit). Haavoittuvuusvarotoimenpiteet pyrkivät joko poistamaan haavoittuvuuden kokonaan, tai rajoittamaan vahinkoa joka seuraisi haavoittuvuuden hyväksikäytöstä. Näistä ensin mainittu on huomattavasti mittavampi, koska sen tavoite on estää kaikkien haavoittuvuuksien hyödyntäminen. Jälkimmäinen taas lieventää riskiä haavoittuvuus kerrallaan. (McManus 2004 s. 111 – 112)

Riskien pienennys- ja siirtostrategiat

Riskinpienennysstrategioiden tavoitteena on pienentää riskin todennäköisyyttä tai vaikutusta projektiin, jolloin sen vaikutus voitaisiin jopa hyväksyä. (McManus 2004, s. 114) Tämä onkin todennäköisesti riskinhallinnan alkuvaiheessa käytetyin tapa riskien käsittelyyn, koska välttämisstrategioita ei ole vielä saatu muodostettua, ja omaksuttua osaksi normaalia jokapäiväistä toimintaa. Riskien siirtostrategioilla pyritään siirtämään riski sellaiselle vastuutaholle, joka sen parhaiten saa hoidettua. Riskien jaottelu kategorioihin tulee aiheelliseksi tässä vaiheessa. Jos jako on tehty vastuualueittain, niin riskin kuuluessa useampaan kategoriaan, sen siirto toisen vastuutahon alaisuuteen voi olla hyvinkin toimiva ratkaisu. Tähän toisaalta voi liittyä myös ongelmakohtia. Tehtävien siirtäminen toisille osapuolille saattaa vääristää henkilöiden tai tiimien tehokkuuksia, vaikka itse riski saataisiinkin siten tehokkaammin ratkaistua. Lisäksi sopimustekniset asiat voivat vaikuttaa tähän, esimerkiksi voidaanko riski siirtää alihankkijan hoidettavaksi, jos riski kohdistuu salassa pidettävään tietoon. Riskien arvioinnin yhteydessä voidaan jo tehdä päätöksiä siitä, kenen vastuulla lähtökohtaisesti minkäkin riskin selvittäminen on. (McManus 2004, s. 112 – 113)

Jäänneriskistrategiat

Vaikka aiemmin mainitut strategiat olisivatkin käytössä, saattaa jäljelle jäädä silti riskejä, joita ei saada kokonaan poistettua. Tavoitteena kuitenkin on, että näiden riskien vaikutukset ovat erittäin pieniä projektille. Näin ollen saattaa olla turhaa käyttää resursseja niiden poistamiseen tai entuudestaan pienentämiseen. Voi hyvinkin olla tehokkaampaa vain puuttua asiaan riskin realisoituessa. (McManus 2004, s. 115)

2.4.6 Riskien valvonta

Riskinhallintasuunnitelman tulee sisältää tiedot valvonnan frekvenssistä sekä valvonnan vastuista. Valvonnan tulee olla osa rutiinia ohjelmistoprojektissa. Riskien valvonta on tärkeää, koska vaikka sen todennäköisyys ja vakavuus voitaisiin ennustaa hyvinkin tarkkaan, mahdollinen tapahtuma-aika ei ole tiedossa. Projektin aikaisessa vaiheessa tehdyt yleistykset eivät välttämättä (ja usein) enää päde ajan myötä. Riskien valvontaa tehdään, jotta sekä ennustettavissa olevat, että tuntemattomat riskit saataisiin estettyä muodostumasta konkreettisiksi riskeiksi. (McManus 2004, s. 123)

Riskien valvontaa voidaan tehdä sen jälkeen, kun edellisessä kohdassa esitellyt riskien lievennysstrategiat ja – menetelmät on otettu käyttöön. Valvonnan tavoitteena on tarkistaa, ovatko tehtyjen päätösten seuraukset suunniteltuja, löytyisikö etsimällä mahdollisuuksia tarkentaa tai muuttaa tarvittavia tietoja riskien lieventämistoimenpiteissä ja kerätä tietoa tulevaisuutta varten, jotta silloin on enemmän tietoa käytössä vanhojen ja uusien riskien lieventämiseen. (McManus 2004, s. 123)

Riskienvalvontaprosessia kehitettäessä on otettava huomioon seuraavia asioita (McManus 2004, s. 123):

- Riskien valvontaan käytettävissä olevan henkilöstön määrä ja resurssit
- Arvio valmistelevan työn määrästä, joka tarvitaan tämän vaiheen aloittamiseen
- Selvitettävien asioiden laajuus (pohjatyöksi ja valvonnan aikana)
- Prosessin laajuus organisaatiossa
- Ulkopuolisten osapuolten määrä ja osallistuminen projektiin
- Osallistujien fyysinen sijainti, esimerkiksi ulkomailla, tai ulkoistaminen
- Välimatkojen tuoma lisäaikavaatimus päätöksentekoon ja konsultaatioon
- Prosessin aloitus- ja lopetustoimenpiteistä päättäminen
- Raporttien ja dokumentaation vaatima aika
- Raportteihin ja dokumentaatioon liittyvään kommentointiin liittyvien henkilöiden lukumäärä

Kuten McManus (2004 s. 124) kirjoittaa, on organisaatiossa huolehdittava siitä, että riskienhallintaprosessi on riittävän erillään varsinaisesta sen valvomasta projektista. Projektipäällikön, tai suurissa projekteissa erikseen määrätyn riskipäällikön, tulee pitää huoli siitä, että riskienhallinta tai mahdolliset havaitut riskit eivät vaikuta suoraan varsinaiseen projektiin ja sen tavoitteisiin, esimerkiksi ohjaamalla kehittäjät tietynlaisiin

toimintatappoihin ”varmuuden vuoksi”. Tällöin saatetaan joutua harhaan projektin varsinaisista tavoitteista.

Riskien valvontaa suorittavan henkilöstön tulee omata käsitys kaikenlaisista projektia uhkaavista riskeistä. Seuraavat aktiviteetit tulee pitää mukana prosessissa, jotta riskejä saadaan lievennettyä (McManus 2004 s. 125):

- Jaksottaisten raporttien seuraaminen projektin varsinaisia tavoitteiden saavuttamisen varmistamiseksi
- Projektin etenemiseen tarvittavan tiedon tarjoaminen asianomaisille
- Riskienhallintahenkilöstön osallistuminen projektiin liittyviin palavereihin tiedon kulkemisen varmistamiseksi
- Projektin kokonaiskuvan tarkastelu suunnitellun jatkon kannalta
- Projektitiimin valvominen työn suunnitellun etenemisen varmistamiseksi
- Projektin katselmusten ja testauksen tulosten tarkastelu asiakasvaatimusten noudattamisen varmistamiseksi
- Muutoshallintaa ja projektin rakenteen valvominen ja organisaation virallisen linjan noudattaminen

Vaikka riski kuuluisi esimerkiksi yhteistyökumppanin tai alihankkijan vastuulle, tulee projektiorganisaation ottaa huomioon mahdollinen tarve kyseessä olevan riskin lieventämiselle. (McManus 2004 s. 125)

2.5 Agenteqin toiminta

2.5.1 Tampuuri-toiminnanohjausjärjestelmä

Agenteqin merkittävin ohjelmistotuote on Tampuuri-verkkopalvelu. Tampuurilla ja siihen yhteydessä olevilla erillisillä palveluilla asiakkaat hallinnoivat liiketoimintansa kannalta tärkeää kiinteistöihin ja asumiseen liittyvää tietoa. Asiakaskunta sisältää vuokrataloyhtiöitä, kaupunkeja, isännöitsijätoimistoja, huoltoyhtiöitä sekä muita kiinteistöalalla mukana olevia toimijoita. Tampuurilla ylläpidettäviin tietoihin lukeutuvat esimerkiksi kiinteistöjen ja huoneistojen asukastiedot ja reskontrapuoli, kiinteistöjen remonttitiedot, muutot, vikailmoitukset ja huoltokalenterit. (Talokeskus 2014)

Asiakkailla on oma tilinsä Tampuurin käyttämiseen, ja joillain asiakkailla on myös oma installaationsa. Ylläpidettävänä on monta eri installaatiota, jotka ovat mahdollisesti eri ohjelmistoversioissa. Lisäksi myös tietokantoja on useita. Asiakkaalla on myös omassa käytössään erilaisia käyttäjäryhmiä, joiden käyttöoikeuksia Tampuurin sisällä hallitaan. Tampuuri ja sen sisältämät moduulit ovat myös erittäin pitkälle konfiguroitavia, riippuen asiakkaan tilaamista ominaisuuksista. Osa asiakkaista hallinnoi kaikkia tarpeellisia tietojaan Tampuurin avulla, mutta osa käyttää lisäksi myös muiden toimittajien järjestelmiä. Näiden asiakkaiden osalta erittäin tärkeässä liiketoiminnallisessa roolissa ovat liittymät, joiden kautta asiakkaan dataa siirretään ulkoisesta järjestelmästä

Tampuuriin ja päinvastoin. Ulkoisissa järjestelmissä käytetään useita erilaisia tiedonsiirtotapoja.

2.5.2 Agenteqin projektit

Agenteqissa on kahdenlaisia projekteja. Käyttöönottoprojektit liittyvät Tampuurin käyttöönottoon uusille asiakkaille, kehitysprojektit ovat nykyisten asiakkaiden tilaamia lisäominaisuuksia Tampuuriin. Käyttöönottoprojektit käynnistyvät, kun yrityksen myynti tekee sopimuksen asiakkaan kanssa. Käytännössä asiakas on käyttänyt jotain muuta järjestelmää vastaavien asioiden tekoon aikaisemmin, ja tämän perusteella asiakkaalla on tiedossa tarpeet, jotka Tampuurin tulee heillä täyttää. Tehdyn sopimuksen perusteella muodostetaan projekti, johon osoitetaan projektipäällikkö. Projektipäällikön tehtävänä on käydä läpi asiakkaan kanssa lopulliseen tuotteeseen tulevat ominaisuudet, määritellä ne, ja saattaa nämä tiedot eteenpäin tuotannolle, jossa ne aikanaan toteutetaan ja toimitetaan asiakkaalle.

Käyttöönottoprojektien vaatimukset projektiorganisaatiolta voivat vaihdella suuresti, riippuen asiakkaan koosta ja heidän tarpeistaan. Pienet huoltoyhtiöt saattavat tarvita vain perustoiminnot, jolloin riittää, että asennetaan vain tarvittavat moduulit ja konfiguroidaan järjestelmä kuntoon. Suuremmilla asiakkailla vaatimukset saattavat olla huomattavasti monimutkaisemmat. Kommunikoinnin eri moduulien välillä tulee toimia luotettavasti, tietojen tulee siirtyä yhteistyökumppaneiden Tampuureihin, ja asiakkaalla saattaa olla erityistarpeita verrattuna Tampuurin aikaisempaan toteutukseen. Esimerkkinä tällaisesta erityistarpeesta on esim. soluhuoneiston huoneiden erottelu toisistaan.

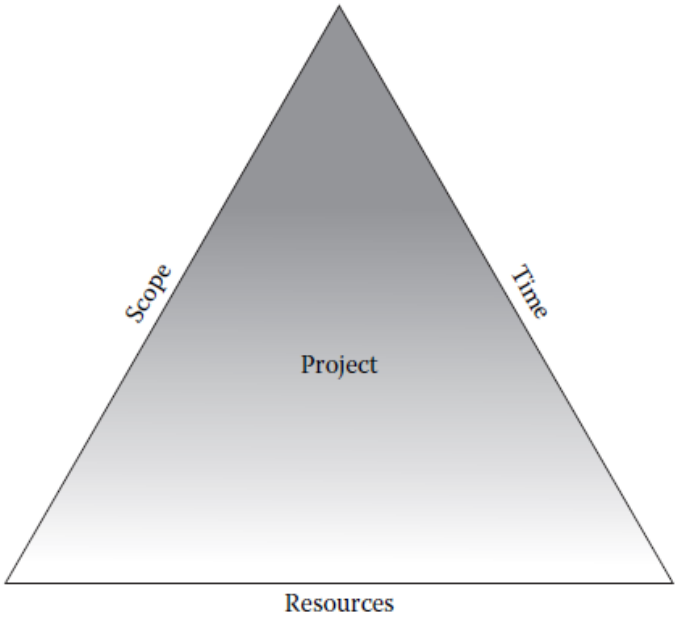
Kehitysprojektissa asiakas saattaa haluta suurenkin uuden kokonaisuuden Tampuuriin. Kyseessä saattaa olla kokonaan uusi asia, termistö ja käyttötarkoitus, mihin projektihenkilöstö ei ole aiemmin tutustunut, on projekti ja sen haasteet aivan erilainen kuin käyttöönottoprojekti, jossa ”vain” räätälöidään Tampuurista asiakkaan tarpeisiin sopiva versio.

Tässä työssä käsitellään Agenteqin toimintaa laajemmalla tasolla kuin vain varsinaisten projektien osalta. Luvussa 4 esitellään prosessit, joista käytännössä Agenteqin toiminta koostuu. Yksi näistä prosesseista sisältää myös tämän kohdan alussa mainitun varsinaisen projektin läpikulun. Syy prosessikohtaiseen näkökulmaan on se, että näin saadaan otettua riskinhallinnan piiriin huomattavasti kattavampi osa yrityksen toimintoja. Prosessit ja projektit kuitenkin liittyvät toisiinsa merkittävästi, mukaan lukien samat osapuolet tuotehallinnassa ja tuotantotiimeissä. Koska Agenteqin toiminnassa samat tekijät ovat osallisena erilaisissa prosesseissa, erilaisilla aikatauluilla, eivät projektiprosessitkaan etene niin sanotusti perinteisesti samalla henkilöstöllä alusta loppuun. Agenteqilla on käytössä ketterä Scrum-menetelmää mukaileva toimintatapa, jolloin ei ole ollenkaan varmaan, milloin mikäkin osa projektia tai prosessia lopulta tehdään, ja kenen toimesta.

Agenteqin ketterällä ja varsin monimutkaisella toimintatavalla suurin pullonkaula kohdistuu tuotehallinnan ja resursoinnista vastaavan tahon kohdalle.

Resursoinnissa yleisesti on merkittävässä roolissa projektinhallintakolmio. Se kuvaa jokaisen projektin koostuvan kolmesta eri osa-alueesta, joista yksi on pääasiallinen tavoite, ja kaksi muuta tulee asettaa siten, että tärkein tavoite saadaan täytettyä. Kolmio on esitetty kuvassa 2.5., jossa englanninkielisiä vastineita suomeksi vastaavat aika (time), lopputulos (scope) ja resurssit (resources). ”Scope” tarkoittaa konkreettisesti laajuutta, mutta tässä se suomennetaan tarkoittamaan käytännössä projektin lopputuloksen laatua. Joissain lähteissä resurssien tilalla käytetään suoraan termiä hinta (cost) (McGhee & McAliney 2007, s. 74), mutta projektinhallinnallisesti se tarkoittaa samaa asiaa, koska yritykselle projektin kustannukset koostuvat henkilöstön työajasta ja kiinteistä resursseista (laitteistot, yhteydet).

Agenteqin jokapäiväisessä toiminnassa tulee vastaan tilanteita, joissa kolmioissa on eri tehtävissä eri painotukset. Esimerkiksi asiakas tarvitsee tuotteeseensa muutoksia nopealla aikataululla lainsäädännön muutosten takia. Tällöin työlle voi olla tiukka aikaraja, ja resursseja lisätään ja vaatimuksia karsitaan sen verran, että tarvittava minimitoteutus on valmis aikarajaan mennessä. Vastaavasti kiireellisempi tehtävä voi siirtää keskeneräisen työn aikataulua, koska se on kerrannaisvaikutuksiltaan yritykselle parempi ratkaisu kuin merkittävä resurssien lisääminen nopealla aikataululla. Onnistuessaan tässä diplomityössä kehitetty riskinhallintamalli auttaa hallitsemaan ja pienentämään projektinhallintakolmioon tulevia muutoksia Agenteqin eri prosessien aikana.



Kuva 2.5. *Projektinhallintakolmio (Gentile 2006, s. 173)*

3 RISKINHALLINTATEORIAN SOVELTAMINEN

3.1 Agenteqin toiminnan asettamat vaatimukset

Lähdettäessä muodostamaan Agenteqille sopivaa riskinhallintastrategiaa on huomioitava yrityksen ominaispiirteitä, jotka rajoittavat käytössä olevia mahdollisuuksia. Agenteqissa projektipäälliköt ovat enemmänkin tekemisissä asiakasrajapinnassa, ja toimittavat kehitettävät tehtävät kehitystiimeille. Toiminnallinen määrittely suunnitellaan yhdessä kehitystiimin kanssa. Täten projektipäälliköt eivät ole tekemisissä varsinaisesti kehitystiimin kanssa.

Scrum-menetelmän ollessa käytössä, luvussa 2 esitettyjen riskinhallintamenetelmien projektipäällikköä vastaavaan tahon muodostavat scrum master ja product owner, jotka sprinttien aikana valvovat tiimin toimintaa ja ohjaavat tiimiä esimerkiksi yllättävien tilanteiden sattuessa. Product owner on Scrumin vastine tuotepäällikölle, ja hänen vastuullaan on tuotteen kehittämisen ja kehitystiimin työn tuloksen maksimointi. Scrum masterin tehtävä on pitää huoli siitä, että Scrumin menetelmiä ja sääntöjä noudatetaan tiimin toiminnassa. (ScrumGuides 2014)

Nykyisellään Agenteqissa riskinhallinta toimii käytännössä niin, että realisoituneiden riskien perusteella pyritään jatkossa minimoimaan saman riskin uusiutuminen. Koska minkäänlaista riskitietokantaa tai -rekisteriä ei ole käytössä, on riskienhallinta täysin opittujen tapojen ja menetelmien, tai tiettyjen henkilöiden vastuulla.

Käytössä olevasta Scrum-menetelmästä on riskinhallinnan kannalta se hyöty, että projektiorganisaatio ja työmenetelmät pysyvät samanlaisina. Tällöin riskinhallinta on helpompi pitää hallinnassa. Luvussa 2 kuvatut riskinhallintamenetelmät perustuvat ajatukseen perinteisemmistä projekteista, joiden koko elinkaari on käytännössä tuotantotiimin käsissä, ja tilanne on usein erilainen verrattuna aikaisempiin projekteihin. Scrum-mallin ollessa käytössä tilanne pystyy kehitystiimin kannalta varsin muuttumattomana projektista ja sprintistä toiseen. Projektipäällikkö ja/tai tuotepäällikkö tekevät toiminnallisen määrittelyn linjaukset asiakkaan kanssa käytyjen keskustelujen pohjalta, ja kun tehtävä tuodaan sprintille, määrittelee ja toteuttaa tuotantotiimi sen annettujen reunaehtojen mukaisesti. Toisin kuin perinteisessä projektimallissa, tuotantotiimin jäseniä ei ole välttämättä mukana määrittelemässä tehtävää. Tämänlainen prosessimalli sisältää paljon sisäänrakennettuja riskejä jo siitä syystä, että asiakas ja prosessin tekijät ovat niin eriytettyjä toisistaan.

Selkeä raja kehitystiimin ja tuote- sekä projektipäälliköiden välissä selkeyttää koko riskinhallinnan lähtökohtia. Tuotantotiimin kannalta on selkeää, kun tehtävät tulevat ”ulkopuolelta”, ja esimerkiksi määrittelyjen ollessa puutteellisia, pyydetään lisätietoja ja siirrytään eteenpäin seuraavana tehtävään. Tuotehallinnan puolella taas voidaan pääsääntöisesti luottaa, että tuotantotiimi tekee sprinteille valitsemansa tehtävät valmiiksi määräaikaan mennessä. Mahdollisten viivästysten ja lisätietotarpeiden osalta tiimi ottaa yhteyttä saman tien, jotta vältytään yllättäviltä tilanteilta.

Riskienhallinnan Agenteqin tapauksessa tekee vaikeaksi se, että vaikka edellä mainitulla tavalla projektissa mukana olevan tahon näkökulmasta kokonaisuus on helposti hallinnassa, kattavan riskinhallinnan ylläpitäminen on haasteellista. Riskien valvontaa suorittavan tahon tai henkilön tulisi tuntea sekä kehitystiimin toimintatavat ja -menetelmät, sekä lisäksi myös tuotehallinnan puolelta jopa välillisesti riskinhallinnan alaiseen projektiin liittyvät uhat. Esimerkiksi projekti- tai tuotepäällikön muiden projektien sekä asiakkaiden tai yrityksen johdon tasolta tärkeämmäksi linjaamien tehtävien toteutuneet riskit voivat aiheuttaa merkittäviäkin hidasteita toiseen käynnissä olevaan projektiin. Tämä vaara on olemassa, vaikka toisen projektin osalta riskinhallinta olisikin ajan tasalla, ja optimaaliset riskinlievennystoimenpiteet olisivat jo tehty.

3.1.1 Yrityskohtaiset rajoitteet riskinhallinnalle

Agenteqin tapauksessa ei ole olemassa henkilöstön jäseniä, jotka voisivat tehokkaasti seurata sekä tuotannon, että tuotehallinnan puolelle jääviä riskejä. Tarvitaan erilliset henkilöt kummankin puolen riskinhallintaan. Tuotantotiimin, eli Scrum-tiimin, kannalta parhaiten asioista on perillä scrum master. Hänellä ei kuitenkaan ole käytännön tietoa tehdyistä ohjelmointiratkaisuista ja Tampuuri-ohjelmiston työn alla olevan osuuden aiemmasta toteutuksesta. Myös varsinaisista kehittäjistä pitäisi jonkun olla tämän takia mukana riskien tunnistamisessa, analyysissä ja suunnittelussa. Riskienhallinta, esimerkiksi riskitietokannan ajan tasalla pitäminen, veisivät näiltä henkilöiltä resursseja. Vaaditut resurssit on kuitenkin jostain otettava, jos ylipäätään riskienhallintaa halutaan käyttää.

Haastetta lisää myös se, että Scrum-mallista johtuen tietty asiakasprojekti ei ole käytännössä koko ajan edes työn alla. Määrittelyjen jälkeen voi kulua useita sprinttejä, ja siten kuukausia, ennen kuin kehitystiimi edes ottaa työn alle kyseisen projektin asioita. Kuitenkin myös tuona aikana tulisi projektiin liittyviä riskejä valvoa, joka kuluttaa resursseja vaikka tehtävät eivät konkreettisesti ole edes työn alla. Esimerkiksi ylempää organisaatiosta tuleva paine jonkin projektitehtävän toteutusvaiheen aikataulun siirtämisestä myöhemmäksi, lopullisen määräajan pysyessä samana, saattaa lisätä projektin viivästymiseen liittyvien riskien todennäköisyyksiä merkittävästi.

Hyvä malli voisi olla soveltaa riskinhallintaa erillisesti tuotannon ja tuotehallinnan tasolle. Agenteqin tapauksessa tästä seuraa erittäin haasteellinen tilanne, koska tuotanto ja tuotehallinta toimivat erillään, ainoan varsinaisen kommunikaatiokanavan ollessa tehtävien saapuminen työlistalle. Käytännössä tilanne luo erittäin vaikean lähestymistavan riskinhallinnan käyttöönottoon, koska nämä tahot ovat Agenteqissa varsin eriytyneet johtuen tuotehallinnan painottumisesta asiakasrajapintaan. Agenteqin organisaatiossa näiden yksiköiden päälliköiden yläpuolella on vain yrityksen ylin johto. Riskinhallintaan tarvittaisiin kummankin yksikön toiminnan tarkasti tunteva henkilö, joka saisi käsityksen molempien yksiköiden riskinhallintapäälliköiden tiedotuksista ja raporteista. Jos tämä ylempi henkilöstön jäsen haluaa olla aktiivisesti riskeihin liittyvässä päätöksenteossa ja priorisoinnissa mukana, tarvitsee hän luonnollisesti kattavammat tiedot kohdealueesta. Tämän ongelman voisi ratkaista vaikka pitämällä esimerkiksi viikoittain kokouksia jossa eri yksiköiden riskinhallintapäälliköt toisivat esiin muutoksia oman alueensa riskeistä, ja näiden mahdollisesti muuttuneita todennäköisyyksiä ja vakavuuksia. Näin saataisiin muodostettua aina ajantasaiset projektikohtaiset riskitietokannat.

3.1.2 Yrityksen riskinhallintaprosessi käytännössä

Luvussa 2 esitetyt Sommervillen ja McManusin esittelemät teoriapohjat riskinhallinnalle ovat varsin samankaltaisia. Molemmissa tapauksissa varsinainen riskinhallintaprosessi koostuu neljästä eri vaiheesta (riskien tunnistaminen, riskianalyysi, riskisuunnittelu, eli käytännössä riskien lieventäminen, ja riskien valvonta). McManus (2004) käy kirjassaan läpi huomattavasti tarkemmin myös jokaisen vaiheen varsinaisia konkreettisia tehtäviä ja ”uhrauksia” joihin yrityksen on ryhdyttävä halutessaan ajaa sisään tehokasta riskinhallintaa.

Lähdettäessä selvittämään Agenteqille sopivaa riskinhallintamallia, käytetään lähtökohtana tätä nelivaiheista mallia, ja yritetään saada se sopimaan Agenteqin toimintatapoihin ja organisaatioon. Jo tämän luvun alussa mainituista organisaatiollisista syistä merkittäviä muutoksia luvun 2 riskinhallinnan toteutustapoihin pitää tehdä.

3.2 Riskinhallinnan lähtökohdat

3.2.1 Riskikategoriat ja –tyypit Agenteqissa

Kun Agenteqissa lähdetään toteuttamaan riskinhallintaa, on aluksi selvitettävä minkälaisia riskejä yritys toiminnassaan kohtaa. Tässä diplomityössä tarkastellaan riskienhallintaa lähtökohtaisesti Agenteqin prosessien kannalta. Agenteqin toimintamalleista johtuen projektien ohella tarkastellaan lisäksi myös prosesseja, joita ei voi tarkastella täysin kuten perinteisiä ohjelmistoprojekteja, vaikka kaikki samat

elementit löytyvätkin. Nämä prosessit esitellään luvussa 4. Kohdassa 2.4 luetelluista Sommervillen riskikategorioista Agenteqin tapauksessa projektiriskit ovat oleellisia prosessien ja projektien koko elinkaaren ajan, kun taas tuoteriskit koskevat enimmäkseen tuotantoa. Liiketoimintariskit ovat varsin pienessä osassa. Käytännössä tämän diplomityön käsittelemällä prosessitasolla ei ole yksittäisiä riskejä, joilla olisi merkittäviä liiketoiminnallisia vaikutuksia. Prosessin sisällä riskit vaikuttavat enemmän kyseisen prosessin tehokkuuteen.

Sommervillen kohdassa 2.4.2 määrittelemät riskityypit jakautuvat eri prosessien alle ja henkilöstön eri tahojen vastuualueille. Agenteqin tapauksessa projektien ja prosessien voidaan ajatella jakautuvan karkeasti kahteen osaan: tuotehallintaan, jossa asiakasrajapinnassa toimivat tuotepäälliköt ja projektipäälliköt vievät työtehtävät tuotantotiimille toteutettavaksi, sekä tuotantoon, jossa eri Scrum-tiimit toteuttavat tuotehallinnassa määriteltyjä tehtäviä sprintti kerrallaan. Riskinhallintaa lähdetään luvussa 4 luomaan juuri tämän tyyppiseen jakoon perustuen.

Riskityypeistä teknologiariskit ja työkaluriskit keskittyvät pääasiassa tuotantotiimeihin. Vaikka tuotehallinta käyttää samoja tietojärjestelmiä tehtävien seuraamiseen ja ylläpitoon, varsinainen lopputuloksen tuottaminen tapahtuu tuotantotiimien käyttämillä työkaluilla. Agenteqin tuottamien verkkopalvelujen luonteesta johtuen, teknologiariskien huomioonottaminen ja niiden minimointi on jo nykyisellään Agenteqissa arkipäivää. Tuotteita voi olla useita eri installaatioita ja julkaisuversioita useilla eri asiakkailla. Se lisää kompleksisuutta riskinhallintaan, ja sen takia riskinhallinta pitäisikin saada irrotettua varsinaisista tuotannon työtehtävistä.

Scrum-menetelmästä johtuen tavoitteena ja käytäntönä on, että tuotantotiimissä mikään tehtävä ei vaadi nimenomaan yhden tietyn työntekijän työpanosta, vaan esimerkiksi tehtävää tekevän henkilön sairastuessa tiimin muut jäsenet voivat ottaa häneltä työn alle jääneen tehtävän hoitaakseen. Tästä syystä henkilöriskit eivät ole niin kriittisiä tuotantotiimeille, vaikka luonnollisesti kokeneempien avainhenkilöiden korvaaminen erityisesti lyhyellä varoitusajalla on erittäin haastavaa. Tuotehallinnassa taas kaikki tietyn projektin tietämys on usein tuotepäällikön ja projektipäällikön takana, jotain esimerkiksi näiden henkilöiden pitkä sairasloma olisi erittäin suuri ongelma, ei vain käynnissä olevalle projektille, vaan potentiaalisesti myös asiakassuhteelle.

Organisaatioriskit on epäselvempi riskityyppi, koska yksittäisen projektin organisaatiorakenne voi olla erittäin monitahoinen. Ja tämä on ongelmallista siksi, että eri tuotantotiimien vastuualueet tuotteiden toteutuksessa ovat pääsääntöisesti täysin erilliset, jolloin toisen tiimin asioista ja mahdollisista ongelmista ei ole mitään käytännön tietämystä. Tästä aiheutuu suuri väärinkäsitysten mahdollisuus ja mahdollisesti muitakin kommunikaatio-ongelmia, tuotehallinnan ollessa yhteydessä eri tiimeihin eri asioissa. Vaatimusriskit ovat selkeästi tuotehallinnan asia, koska Scrum-mallissa on

tarkoituksenmukaista, että tuotepäälliköltä, product owner, tulee sprintille valmiiksi määriteltyjä tehtäviä, jotka voidaan sprintin aikana tehdä ilman tarvetta lisätiedoille.

Arviointiriskit ovat myös pitkälti molempien puoliskojen alueella. Tuotantotiimien pitäisi pystyä määrittelyjen perusteella arvioimaan tehtävien työaika-arvioita siinä määrin, että osataan valita oikea määrä tehtäviä sprinteille. Tämän arvion pitäisi olla niin tarkka, että tuotehallinnassa voidaan luottaa tehtävän valmistuvan luvattuna aikana. Tuotehallinnassa taas ongelmana on arvioida lähitulevaisuuden työruuhkaa, jotta asiakkaan kanssa osattaisiin sopia realistisia aikatauluja, mutta myös samalla asiakasta mahdollisimman hyvin palvellen. Lisäksi tuotehallinnassa on palveluiden eri moduulien tekniseen toteutukseen perehtymättömänä käytännössä mahdotonta arvioida esimerkiksi uusien ominaisuuksien toteutuksen vaatimaa työmäärää.

3.2.2 Riskinhallintaorganisaatio

Henkilöstön toimenkuvat

Kuten edellä on kuvattu, Ageteqin toiminta eivät vastaa täysin perinteisen ohjelmistokehityksen projekteja. Projekteihin ei varsinaisesti dedikoida projektitiimiä, joka määrittelisi ja toteuttaisi projektin asiakasvaatimusten mukaan alusta loppuun. Agenteqinssa on tuotannossa käytössä Scrum-menetelmä, johon tuotepäälliköt tuovat sprinteille tehtäväksi priorisoimiaan tehtäviä. Osa tehtävistä on heidän itsensä asiakkaalta saamia, osa projektipäälliköiden kautta tulevia varsinaisiin asiakasprojekteihin liittyviä tehtäviä.

Näinollen riskienhallintaa ei käytännössä kannata mahdollisimman laajan hyödyn saavuttamiseksi suunnitella ja soveltaa projektikohtaisesti, vaan laajemmin, Agenteqin toiminnan eri osa-alueisiin. Yrityksen käytännöistä seuraa myös se, että projektipäällikkö ei johda projektia tuotannon näkökulmasta, vaan enemmänkin asiakkaan näkökulmasta. Agenteqissa projektipäällikkö on kyllä tärkeässä osassa toiminnallista määrittelyä, ja käytännössä asiakkaan kanssa käy läpi asiakasvaatimukset ja neuvottelee niistä toteutuksen ja olemassa olevan järjestelmän kannalta oleellisen kokonaisuuden.

Perinteisen ohjelmistoprojektin projektipäällikön tehtäviä hoitavat Agenteqissa myös tuotepäälliköt ja scrum masterit. Tämä on suuri haaste riskinhallinnassa, koska scrum master on tietoinen tuotantotiimin tehtävistä ja niiden etenemisestä, mutta ei ole tekemisissä tuotehallinnan asioiden kanssa. Lisäksi scrum master on kyllä tehtävätasolla perillä tuotannon töistä, mutta ei välttämättä omaa tuntemusta varsinaiseen tietyn ominaisuuden ohjelmoimiseen. Täten srcum master ei välttämättä voi ottaa osaa esimerkiksi työmääräarvioiden tekemiseen. Tuotepäällikön näkymä taas päättyy sprint planningeihin, jossa käydään sprinteille otettavat tehtävät läpi. Tämän jälkeen tuotepäällikkö teoriassa vain odottaa, että sprintin tehtävät ovat sprintin päättyessä

valmiit. Käytännössä hän kuitenkin tarjoaa tarkennuksia tehtävien määrittelyihin epäselvyyksien ilmetessä. Projektipäällikön ja tuotepäällikön tehtävät ovat osittain lomittaiset, molemmat ovat asiakkaan kanssa tekemisissä, mutta eri tehtävien osalta. Näin ollen kumpikaan heistä ei yksinään voi olla perillä kaikista tuotehallinnan asioista tiettyyn asiakkaaseen liittyen. Riskinhallinnan kannalta tästä syystä on käytännössä pakko käsitellä erillisinä projektipäälliköiden ja tuotepäälliköiden tehtävät, ja siten myös niiden riskinhallinta.

Teoriaosuudessa painotetaan paljon riskinhallintaprosessin vaatimaa resurssimäärää. Tämä on oleellinen asia myös Agenteqin tapauksessa. Asioista parhaiten perillä olevat henkilöt ovat erittäin työllistettyjä, ja kehitystiimeilläkin riittää koko ajan paljon tehtävää. Muutenkin yritystasolla kasvu on ollut nopeaa, joten ”hiljaisempia kausia” ei ole odotettavissa. Näin ollen Agenteq on malliesimerkki siitä, miten yrityksen johdon on päätettävä halutaanko riskinhallintaan panostaa merkittävästi. Tämän takia on tärkeää tuoda riskinhallinnan tarpeet ja perusteet päätöksentekijöiden tietoon, jotta riskinhallintaan panostamisen hyödyt ja haitat voidaan perusteellisesti käydä läpi. Päätöksen tekeminen ei missään tapauksessa ole helppoa, koska hyödyt tulevat esiin vasta pidemmällä aikavälillä, ja aluksi riskinhallintaan panostaminen lisää huomattavasti monen eri tahon työmäärää valmistumista odottavien työtehtävien kustannuksella.

Resursseja ei kuitenkaan kulu vain varsinaisten riskien arviointiin ja minimointiin. Jotta pitkällä tähtäimellä saadaan koko yrityksen laajuudella parannettua toimintaa, täytyy riskinhallinta ottaa osaksi yrityksen strategiaa jopa laajemmin. Saadakseen tulevaisuudessa poistettua ja minimoitua riskejä jo ennen projektin riskinhallintatoimenpiteitä, tulee yrityksen panostaa myös tiedon jakamiseen niin, että tietämystä saadaan välitettyä koko organisaation läpi kaikille tahoille. Tavoitteena kuitenkin on, että riskinhallintahenkilöstön ulkopuolinen työntekijä osaa tulevaisuudessa soveltaa aiempien projektien riskeistä opittuja asioita ja käytännön työssään tehdä riskien lievennystä. Tästä esimerkkinä voisivat olla ohjelmointityössä monikäyttöisten ja toimivaksi todettujen komponenttien käyttö uuden testaamattoman ohjelmakoodin sijaan tai asiakkaan tukipyyntöjä kirjattaessa yhtenäisen rakenteen käyttö ongelman kuvausta kirjoittaessa.

Riskinhallintatiimin vastuujako

Kuten edellä on todettu, tulee riskinhallinnan kattaa erittäin laajasti erilaisia osa-alueita Agenteqin sisällä. Käytännössä riskinhallinnan tulee alkaa jopa myyntitilanteesta, koska jo tuolloin myytäviä ominaisuuksia ja aikatauluja luvatessa on oltava tietoinen koko organisaation riskitilanteesta. Agenteqissa projektipäälliköt ovat osallisena sopimusten sisällön määrittelyyn, joten projektien alkuvaiheessa projektipäälliköt ovat kykeneviä arvioimaan riskien tilannetta. Tuotepäälliköillä on vastaava tilanne, vaikka eivät suoranaisesti varsinaisten projektien kanssa olekaan tekemisissä. Pienimuotoisemmat

työtilaukset sisältävät samat piirteet riskinhallinnallisesta näkökulmasta. Näiden kahden oleellisen henkilön lisäksi riskinhallintaorganisaatiossa tarvitaan henkilöitä tuotannon puolelta. Vaikka tuote- ja projektipäälliköt eivät olekaan toisten saman nimikkeen henkilöiden kanssa samoissa projekteissa, heidän toimintamallinsa asiakkaan ja kehitettävän tuotteen suhteen ovat samanlaiset. Näin ollen riskinhallinnan kannalta syvällistä tuntemusta juuri tietyn projektin tai asiakkaan tietoihin ei vaadita riskien arvioimiseksi ja käsittelemiseksi.

Koska eri tiimien tehtävät eroavat toisistaan niin merkittävästi, tarvitaan käytännössä tuotannon jokaisen tiimin tehtäviä tunteva henkilö osaksi riskinhallintaa. Tiimien käytännöt eroavat toisistaan jonkin verran, ja kaikki tiimit eivät edes työskentele saman Tampuuri-tuotteen kanssa. Tällöin henkilöllä ei välttämättä ole mitään tuntemusta toisen tiimin tehtävien kohteeseen liittyen. Riskinhallintaorganisaatioon kuuluminen ei kuitenkaan välttämättä tarvitse tarkkaa tuntemusta ohjelmakoodista, joten siinä mielessä scrum master saattaisi olla sopiva hoitamaan tehtävää. Tämä kuitenkin vie luonnollisesti paljon resursseja vastuullisen ja tärkeän tehtävän omaavilta scrum mastereilta.

Jotta Agenteqin riskinhallintaprosessin voidaan olettaa olevan tarpeeksi kattava koko prosessin elinkaaren ajan, tarvitaan riskinhallintaorganisaatioon vähintään yksi projektipäällikkö ja yksi tuotepäällikkö. Näiden lisäksi mukana tulisi olla ainakin yksi scrum master, jolla on käsitys tiimin sisäisestä organisoinnista, ja lisäksi myös ylempää yrityksestä tulevista resurssointikäytännöistä. Näiden lisäksi tarvitaan joitakin henkilöstön jäseniä, jotka työskentelevät joko tuotannossa tai asiakaspalvelussa. Tavoitetilanteessa jokaiselle riskinhallintaorganisaation osapuolelle riskinhallinta on vain pieni osa työpanoksesta, ja se saadaan integroitua normaalien työtehtävien oheen. Tällä ryhmällä voi esimerkiksi olla yhteisiä viikoittaisia katselmuksia, joiden välillä he itsenäisesti käyvät läpi oman ”vastuualueensa” riskitilannetta. Tämän lisäksi tulee vielä sitten haasteellinen vaihe kerätyn tiedon jakamisesta muulle henkilöstölle organisaatiossa. Tiedon jakamisen kautta tietämys integroidaan osaksi yrityksen toimintatapoja ja strategiaa.

3.2.3 Riskinhallinnan pitkän tähtäimen suunnitelma

Agenteqin tapauksessa riskinhallinnan pitkän tähtäimen suunnitelma on siinä mielessä haasteellinen, että samaa kaavaa ei voi soveltaa täysin erilaisiin osiin organisaation toimintaa. Aikaisemmin todettiin riskityyppien jakaantuvan paikoittain erittäin selkeästi eri osiin yrityksen toimintaa, joten toisaalla organisaatiossa sovelletaan tietynlaisia lievennysmenetelmiä ja muualla taas täysin erilaisia. Täytyy kuitenkin pyrkiä siihen, että oli paikka Agenteqin organisaatiokaaviossa tai prosesseissa missä tahansa, täytyy riskiin suhtautua aina riskinä, ja tarvittaessa jopa ”nöyrästi”. Luonnollisesti jokaisen löydetyn riskin vakavuuden ja todennäköisyyden pystyy määrittelemään luotettavasti vain

kyseessä olevan riskityypin vaikutusalueen tunteva henkilö, mutta prosessi, jolla riskejä etsitään, tulisi silti olla jokaisen riskin kohdalla sama.

Lähtökohtana systemaattisen riskiseulonnan rakentamiselle voisi olla esimerkiksi riskien jako kategorioittain (kohdassa 2.4 mainitut projekti-, tuote- ja liiketoimintariskit). Tämän jälkeen listataan käsiteltävän prosessin eteneminen vaiheittain jokaisen kategorian osalta. Kun kyseisen osa-alueen tunteva riskinhallintaorganisaation jäsen on käynyt läpi ko. kategorian riskit, pitää vielä verrata löydettyjä riskejä riskitietokannan vastaaviin tietoihin. Jos projektissa ilmenee riski, jota ei ole osattu ottaa huomioon riskejä kartoitettaessa, tulee riski kuitenkin lisättyä tietokantaan ja myös analysoitua. Täten, kun vastaavan tehtävän riskejä seuraavassa projektissa etsitään, tulisi aiemmin kesken projektin löydetty riski olla dokumentoitu niin, että tämän historiatiedon perusteella se osataan seuraavalla kerralla ottaa ajoissa huomioon.

Riskitietokannan toteutus on tässä asiassa suuressa osassa. Historiatietoon vertailun tulee olla sujuvaa ja tehokasta, koska riskien huolellinen kartoittaminen on muutenkin paljon resursseja vaativaa työtä, ja hätiköinti saattaa kostautua pahasti. Tehokas toiminta vaatii myös riskinhallintatiimiltä tehokasta sisäistä organisointia, jotta kaikki tarvittavat osa-alueet käydään läpi tehokkaasti, mutta turhaa päällekkäistä työtä välttäen. Ehkä suurimpana haasteena kattavan riskilistan saamiseksi on edellä mainittujen vaihe vaiheelta etenemisen ja historiatietoon nojaamisen lisäksi vaadittu uusien riskien etsiminen. Vaikka tuntuisikin siltä, että uusi projekti sisältää samat riskit kuin aiemmin toteutettu vastaavanlainen kokonaisuus, tulee uusia riskejä etsiä siitä huolimatta aivan kuten ensimmäiselläkin kerralla. Mitä myöhemmin riski havaitaan, sitä kalliimmaksi sen minimointikustannukset tulevat. Tämä ei päde pelkästään uusiin riskeihin, vaan myös aiemmin löydettyihin riskeihin ja niiden todennäköisyyksiin ja vakavuuksiin. Ero samankaltaisen projektien riskien ominaisuuksien välillä voi olla kiinni erittäin näennäisesti pienistä yksityiskohdista, esimerkiksi ajoittuminen tunnettuun influenssa-aikaan, kehitystiimin kokoonpanon muutokset aiempaan verrattuna, asiakkaiden keskinäisen prioriteetin muuttuminen yrityksen silmissä tai uusi yhteyshenkilö asiakkaan puolella.

3.2.4 Projektin ja riskinhallinnan aloittaminen

Projektien alkaessa, ja jopa ennen sitä, tulee asettaa projektin tavoitteet ja onnistumiskriteerit. Riskinhallinta perustuu oleellisesti näihin, mutta ne ovat luonnollisesti oleellinen osa projektia jo itsessään. Tavoitteiden ja onnistumiskriteerien kautta voidaan kuitenkin mitata projektin onnistumista, ja niihin voidaan sisällyttää myös riskinhallinnan tuomat vaikutukset. Varsinkin riskinhallinnan käyttöönoton alkuvaiheessa on erittäin oleellista pystyä jotenkin mittaamaan riskinhallinnan yksittäiselle projektille ja koko yritykselle tuomaa hyötyä. Monesti on vaarana, että projekti tehdään aikataulun puitteissa valmiiksi, mutta lähiviikkojen aikana kuitenkin

joudutaan tekemään useita muutoksia, korjauksia ja päivityksiä. Tällaisista asioista, jotka tarkoittavat projektin aikataulun pettämistä, tulisi pitää kirjaa. Jos riskinhallinnalla saadaan näitä lisätöitä vähennettyä, sen pitää myös selkeästi näkyä ilman erillistä analyysiä.

Agenteqin tapauksessa on panostettava mielekkäiden onnistumiskriteerien määrittelyyn. Koska myynnin ja tuotannon välinen kuilu on niin suuri, ongelmaksi muodostuvat helposti liian optimistiset aikataululupaukset asiakkaan suuntaan. Tällöin myynti voi pitää projektin onnistumisena vain ja ainoastaan asiakkaalle myydyn ja luvatun tuotteen toimittamista määräajassa, kun taas organisaatiossa lähempänä tuotantoa voidaan todeta, että asiakkaalle luvatun ominaisuuden toteutus sellaisenaan ei ole mielekästä, vaan kannattaa neuvotella asiakkaan kanssa kehityksen viemistä hieman eri suuntaan. Näin mahdollisesti aiemmin sovitut tavoitteet ja aikataulut saattavat olla pahasti vanhentuneita. Käytännössä projektien tavoitteet tulevat projekti- ja tuotepäälliköiltä. Tuotantotiimit eivät yksinään omaa riittävää tietoa asiakkaista ja heidän sopimuksistaan, eivätkä edes yrityksen sisäisistä tavoitteista, jotta voisivat merkittävässä määrin ottaa kantaa projektitasolla tavoitteiden täyttymiseen.

Varsinaisen projektin tavoitteiden lisäksi on myös määritettävä, mitä riskienhallinnalla halutaan saavuttaa. Tähtäimessä on oltava selkeitä hyötyjä, eikä vain yleistä laadunparannusta. Yksi lähtökohta on miettiä, mikä olisi tilanne, jos nykyisistä projekteista saataisiin tunnetut ongelmakohdat poistettua tai minimoitua heti alussa. Vai onko mahdollisesti nykytilanne se, että lähtökohtaisesti oletetaan projektin etenevän ilman ongelmia, ja riskien realisoituessa sitten joudutaan venymään ja yllämainitut tarkasti määritellyt projektin onnistumiskriteerit eivät täyttyisi. Tarkkoja prosenttilukemia työtehtävien nopeutumisesta ja hidastumisesta on vaikea saada, mutta esimerkiksi jos tuotantotiimien työntekijät pitävät kirjaa siitä, paljonko työaikaa viikkotasolla kuluu erilaisten työkalujen teknisten ongelmien kanssa, voidaan saada tietoa miten ko. asiaan etukäteen puuttumalla saadaan työaikaa valjastettua tehokkaampaan käyttöön. Numeroihin perustuvan tehokkuusmittarin lisäksi riskienhallinnalla voidaan saavuttaa myös abstraktimpia tavoitteita. Varsinainen tehokkuuden parantaminen vaikuttaa myös positiivisesti asiakastyytyväisyyteen; deadlinet pitävät, asiakas voi luottaa sovittujen asioiden paikkansapitävyyteen, eikä heidänkään tarvitse varautua yllättäviin ongelmiin. Tehokkuuden parantuminen vaikuttaa yrityksessä myös sisäisesti. Ikävien yllätysten vähentyessä henkilöstön mieliala nousee, ja muutenkin tulosten parantuessa tunne oman työpanoksen tärkeydestä kasvaa.

3.3 Riskinhallintamenetelmän valinta

3.3.1 Johdanto OCTAVE Allegroon

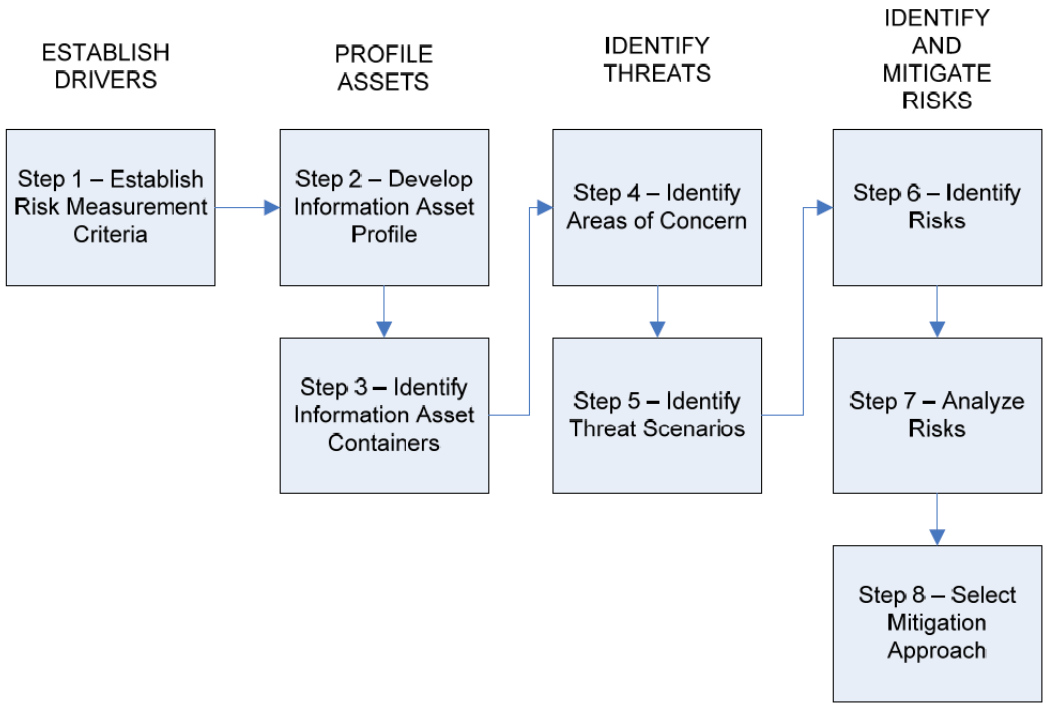
Luvussa 2 esitetyt riskinhallintaprosessin vaiheet ja niiden noudattaminen ei vielä tarjoa mitään konkreettisia käytännön menetelmiä riskienhallinnan toteuttamiseen. Luku 2 kävi vain läpi asiat, joita yrityksen kannattaa kattaa riskienhallinnalla. Luvun 3 kohdat 3.1 ja 3.2 taas toivat esiin Agenteqin ominaisuuksia, jotka asettavat reunaehtoja riskienhallinnan toteuttamiselle.

Tässä diplomityössä suunnitellaan riskinhallintaprosessia nimenomaan Agenteqin tarpeisiin. Tämän takia varsinaisia käytännön menetelmiä muodostettaessa käytetään OCTAVE Allegro –menetelmää (Caralli 2007). Samaa menetelmää on käyttänyt Teemu Keiski opinnäytetyössään Developing Security in the System Developement Lifecycle (Keiski 2013), kartoittaessaan Agenteqin tietoturvariskejä vuosien 2012 ja 2013 aikana.

OCTAVE Allegro –menetelmä sopii Agenteqin tarpeisiin, koska se on räätälöity organisaatioille, joilla ei ole aikaa ja resursseja laajamittaiseen riskiarviointiin. Menetelmä voidaan ottaa käyttöön ilman suurta, valmista, riskinhallintatietoutta, ja se tarjoaa valmiit materiaalit workshop-tyyppiseen toimintaan. (Keiski 2013, s. 55) Keiski (2013, s. 55) huomauttaa, että tämä menetelmä sopii Agenteqille myös siksi, että organisaatiossa ei ennestään ole merkittävää riskinhallintatietoutta. Keiskin tietoturvaprojektin aikana yrityksen johto antoi luvussa 2 tärkeäksi mainitun tukensa riskinhallintamenetelmälle, joten senkin puolesta se on luonnollinen valinta myös tässä projektissa. (Keiski 2013, s. 54) OCTAVE Allegro –menetelmää joudutaan lähestymään hieman eri tavalla ja soveltaen, koska se on suunniteltu tietoturvariskien kartoittamiseen.

3.3.2 OCTAVE Allegro –menetelmän vaiheet

OCTAVE Allegro –menetelmä jakautuu neljään alueeseen. Ensimmäisessä alueessa määritellään riskin mittaamisen kriteerit, jotka sopivat yhteen yrityksen strategisten tavoitteiden kanssa. Alueessa kaksi tunnistetaan ne tietovarastot, jotka sisältävät riskialttiita resursseja. Kolmantena selvitetään uhat, jotka aiheuttavat riskejä vaiheen kaksi tietovarastoille. Kolmas alue vastaa luvussa 2 esitettyä riskien tunnistamista. Viimeisenä alueena on riskien tunnistaminen ja lieventäminen, jotka ovat sisällöltään samat kuin luvussa 2 on esitetty. (Caralli 2007, s. 17) Nämä neljä aluetta on jaettu yhteensä kahdeksaan vaiheeseen, jotka on esitetty kuvassa 3.1. (Caralli 2007, s. 4).



Kuva 3.1. *OCTAVE Allegro –menetelmän vaiheet (Caralli 2007, s. 4)*

Luvussa 4 kuvataan tarkemmin, kuinka OCTAVE Allegro riskinhallintaprosessi etenee vaihe vaiheelta. Menetelmän alueet ja vaiheet mukailevat luvussa 2 esitettyä riskinhallintateoriaa. Kyseessä on uhkasuuntautunut riskinhallintamenetelmä. Tämä tarkoittaa sitä, että prosessi alkaa ”suojeltavien” tietovarastojen, resurssien, kartoittamisesta. Tämän jälkeen näiden tietovarastojen kautta aletaan kartoittamana ensin uhkia, ja sitten uhista muodostuvia riskejä. Riskien jaottelu luvussa 2 esiteltyjen kategorioiden ja tyyppien perusteella on käytännössä OCTAVE Allegron vaihe 1. Tässä menetelmässä tuodaan kyseisen jaottelun lisäksi rinnalle myös priorisointi riskin vaikutusalueen mukaan, ja tätä kuvataan tarkemmin kohdassa 4.3. Muita alkupään vaiheita, eli kuvassa 3.1. esitetyt vaiheet 2 – 5, ei käytännössä ole teoriaosuudessa esitellyissä riskinhallintaprosesseissa.

Luvun 2 teoriassa lähdetään liikkeelle suoraan riskien etsimisestä. OCTAVE Allegron vaiheille 6 – 8 löytyy vastineet suoraan teoriaosuudesta. Näiden vaiheiden jälkeen jää vielä luvussa oleellisena osana mainittu viimeinen vaihe, riskivalvonta. OCTAVE Allegro käsittää vain yhden iteraation riskinhallintaprosessista, joten se ei itsessään tarjoa ohjeita jatkuvaan riskinhallinnan ylläpitoon. Jää yrityksen riskinhallintastrategian varaan määrittää, kuinka usein tämä menetelmä käydään läpi, ja kuinka perusteellisesti.

Koska OCTAVE Allegro -riskinhallinmenetelmä on suunniteltu lähinnä tietoturvariskejä silmälläpitäen, ei menetelmää täsmällisesti noudattamalla saada katettua Agenteqin prosessien riskinhallintaa riittävällä laajuudella. Tämän takia menetelmää pitää soveltaa.

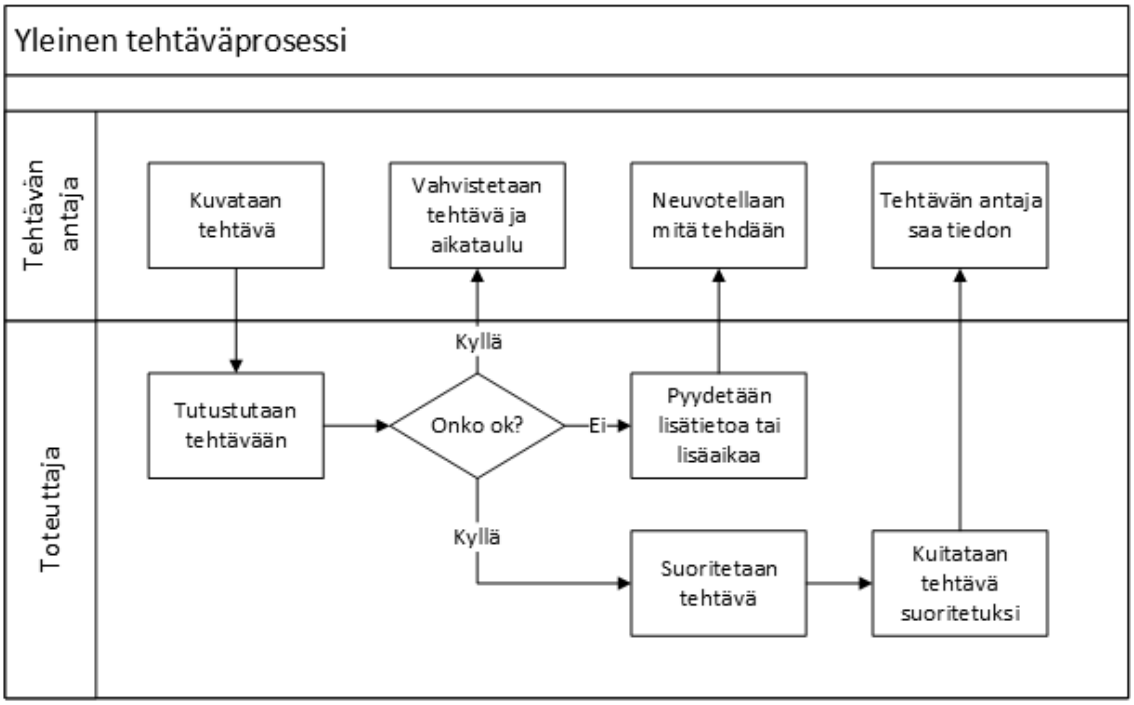
4 UUDEN RISKINHALLINTAMENETELMÄN KÄYTTÖÖNOTTO

4.1 Prosessit

Agenteqin toiminta perustuu vakioituihin prosesseihin. Ohjelmistopalveluja tuottavassa yrityksessä asiakkaan ja työn toteuttavan kehittäjän välissä on monta vaihetta ja tekijää, jotka kaikki ovat oleellisessa osassa riskinhallinnan kannalta. Tässä kohdassa käydään läpi Agenteqin toiminnassa käytössä olevat prosessit, ja niissä toimijoina olevat tahot. Prosessit esitetään kaavioina, ja kaaviokohtaisesti listataan ko. prosessiin osallisena olevat tahot myöhempää käsittelyä varten. Kaaviot kuvaavat tietynlaista prosessia aina juuri kyseessä olevan prosessin omasta näkökulmasta. Joidenkin prosessityyppien välillä esiintyy päällekkäisyyksiä, jolloin ne voivatkin käytännössä sisältyä toisiin prosesseihin.

4.1.1 Yleinen tehtäväprosessi

Tämä prosessi kuvaa erittäin yleisellä tasolla yrityksen prosesseja, ja toiminta tapahtuu vain kahden eri roolin välillä: tehtävän antajan ja toteuttajan. Yleinen tehtäväprosessi on esitetty kuvassa 4.1.



Kuva 4.1. *Yleinen tehtäväprosessi (Agenteq 2014)*

4.1.2 Projektiprosessi

Projektiprosessi kuvaa sen, miten asiakkaan tarpeesta luodaan projekti, toteutetaan se, ja toimitetaan projektin lopputuloksena syntynyt tuote asiakkaalle. Prosessissa osallisena ovat ensin asiakas ja myynti, jonka jälkeen syntymässä oleva projekti arvioidaan tuotehallinnassa (”projektitoimisto”), jonka jälkeen nimetään projektipäällikkö hoitamaan projektia. Tässä prosessissa on ohitettu projektin toteuttamisen tarkempi kuvaus. Projektin toteuttaminen on käytännössä vastaava kuin kohdissa 4.1.3 ja 4.1.4 esitellyissä tuotekehitysprosessissa ja työtilausprosessissa. Projektiprosessi on kuvattu kaaviona liitteessä 2.

Prosessi käynnistyy asiakkaan tarpeen syntymisestä. Myynti laatii sopimuksen ja kerää tiedot projektin sisällöstä. Tämän jälkeen perustetaan projekti, ja projekti siirtyy projektipäällikön hallintaan. Projektipäällikkö pitää yhteyttä asiakkaaseen, sekä suunnittelee ja valmistelee projektin toteutusta varten. Toteutuksen jälkeen projektin lopputulos hyväksytetään asiakkaalla, ja päätetään projekti.

Projektiprosessin oleellisia toimijoita ovat:

- Asiakas
- Myynti
- Tuotehallinta (Projektitoimisto)
- Projektipäällikkö

4.1.3 Tuotekehitysprosessi

Tuotekehitysprosessi kuvaa, kuinka asiakkaan tarve saada esimerkiksi uusi ominaisuus käytössä olevana tuotteeseensa kulkee prosessikoneiston läpi. Kaaviossa nähdään, kuinka prosessin aikana käydään läpi kaksi muuta prosessia, kohdissa 4.1.4 ja 4.1.7 läpi käytävät työtilausprosessi ja versiopäivitysprosessi. Liitteessä 3 esitetystä kaaviosta nähdään, että tässä prosessissa suuri painopiste on tuotepäällikön tehtävissä. Tuotekehitysprosesseina toteutettavat tehtävät ovat usein kooltaan varsin pieniä, joten suuret haasteet tulevatkin resursoinnin ja aikataulun kanssa, kun tuotekehitysprosesseja on useita käynnissä samaan aikaan samojen tuotepäälliköiden ja tuotannon henkilöstön jäsenten takana. Tuotekehitysprosessi on esitetty kaaviona liitteessä 3.

Prosessi käynnistyy asiakkaan tarpeesta. Tuotepäällikkö käy tarpeen läpi, ja tuotekehityksen kanssa päättää lähdetäänkö asiaa viemään eteenpäin. Mahdollisen asiakkaalle tehdyn tarjouksen jälkeen siirretään tehtävä työlistalle prioriteettinsa mukaisesti, josta se aikanaan otetaan työn alle. Valmis työ hyväksytetään asiakkaalla, ja päätetään uuden ominaisuuden käyttöönotosta.

Tuotekehitysprosessin oleellisina toimijoina ovat:

- Asiakas
- Tuotepäällikkö
- Tuotekehitys
- Tuotanto
- Myynti

4.1.4 Työtilausprosessi

Työtilausprosessi kuvaa yksityiskohtaisemmalla tasolla tuotekehitysprosessia. Työtilausprosessissa kuvataan tarkemmin tiedon kulku yrityksen sisällä ja asiakkaan suuntaan, kun suunnitellaan tarjousta ja aikataulua. Työtilausprosessi on kuvattu kaaviona liitteessä 4.

Prosessi käynnistyy asiakkaan tarpeesta. Projektipäällikkö ottaa tarjouspyynnön vastaan, ja selvittää onko kyseessä uusi tuotekehitystehtävä vai ylläpidollinen tehtävä. Selvityksen jälkeen tehdään tarjous, jonka jälkeen sovitaan aikataulutus. Toteutuksen jälkeen asiakasta tiedotetaan ja laskutetaan tehdystä työstä.

Työtilausprosessissa toimijoina ovat:

- Asiakas
- Projektipäällikkö
- Tuotepäällikkö
- Tuotekehitys
- Arkkitehti
- Tuotanto

4.1.5 Asiakastukiprosessi

Asiakastukiprosessi kuvaa asiakkaalta tulevan tukipyynnön kulkemista yrityksen sisällä. Asiakkaan tukipyyntö saattaa olla esimerkiksi heidän havaitsemansa bugi, käyttöopastuspyyntö tai tuotekehitysehdotus. Tukipyynnön luonteesta riippuu merkittävästi, mitkä kaikki osapuolet Agenteqin sisällä ovat osallisena prosessiin. Asiakastukiprosessi on esitetty kaaviona liitteessä 5.

Prosessi käynnistyy asiakkaan tukitarpeesta. Asiakaspalvelu käsittelee viestin, lisää sen tukijärjestelmään, tarvittaessa kysyen lisätietoja. Jos mahdollista, ongelma selvitetään asiakaspalvelussa, muuten käytetään kohdassa 4.1.6 esitettyä bugiprosessia. Kun asia on saatu selvitettyä tai korjattua, hyväksytetään se asiakkaalla, ja prosessi päättyy.

Asiakastukiprosessissa osallisena ovat:

- Asiakas
- Tukipalvelu
- Tukipalvelu linja 2
- Tukijärjestelmä

Jos tukipyynnössä on kyse järjestelmässä olevasta bugista, tapahtuu sen korjaaminen bugiprosessin alla.

4.1.6 Bugiprosessi / Hotfix-prosessi

Bugiprosessi kuvaa järjestelmästä löytyneen bugin korjaamista. Huomattavaa on priorisointi bugin vakavuuden mukaan. Tarvittaessa päivitys tehdään heti asiakkaan järjestelmään kiireisenä päivityksenä. Muuten korjaus menee samalle listalle muiden kehitystehtävien kanssa. Bugi- ja hotfix-prosessi on kuvattu kaaviona liitteessä 6.

Prosessi käynnistyy havaitusta bugista. Jos bugi ei ole kriittinen, siirtyy se kohdassa 4.1.3 käsitellyn tuotekehitysprosessin piiriin. Kriittisen bugin tapauksessa ottaa kehitystiimi korjauksen välittömästi työn alle. Korjauksen jälkeen luodaan päivityssuunnitelma. Asiakasta tiedotetaan päivityksestä, ja läpäistyn testauksen jälkeen prosessi päättyy.

Bugi- ja hotfix-prosessissa osalliset ovat:

- Asiakas
- Asiakaspalvelu
- Sovelluspalvelu
- Kehitystiimi
- Tuotekehitys
- Operaattori

4.1.7 Versiopäivitysprosessi

Versiopäivitysprosessi kuvaa asiakkaan järjestelmän päivittämisen siitä eteenpäin, kun päivitys tai korjaus on kehitystiimin puolesta valmis. Versiopäivitysprosessi on kuvattu kaaviona liitteessä 7.

Prosessi käynnistyy, kun kehitetyt ominaisuudet ovat valmiina päivitettäväksi asiakkaan järjestelmään. Tuotekehitys päättää julkaisusta, ja IT-tiimi suunnittelee ja resurssoi varsinaisen päivityksen. Yksityiskohdista sovitaan asiakkaan kanssa. Ensin tehdään ja testataan mahdollinen testauspäivitys. Mahdollisten virheiden korjaamisen jälkeen tehdään varsinainen päivitys. Onnistuneen tuotantopäivityksen jälkeen asiakas hyväksyy päivityksen, ja prosessi päättyy.

Versiopäivitysprosessissa osana ovat:

- Asiakas
- Asiakaspalvelu
- Sovelluspalvelu
- Testaus
- Kehitystiimi
- Tuotekehitys
- Operaattori/PP

4.2 Osapuolten ryhmittely

Luvussa 4.1 Käytiin läpi prosessit, joista nostettiin esiin jokaisessa prosessissa osallisena olevat tekijät/toimijat. Tässä kohdassa jaetaan nämä ryhmiin, joita käytetään myöhemmin riskinhallintaa suunniteltaessa.

Ryhmä 1:

- Asiakas

Ryhmä 2:

- Myynti

Ryhmä 3:

- Asiakaspalvelu
- Sovelluspalvelu

Ryhmä 4:

- Projektipäällikkö
- Tuotepäällikkö
- Tuotekehitys

Ryhmä 5:

- Tuotantotiimi
- Arkkitehti
- Testaus

Ryhmä 6:

- Tukijärjestelmä
- Operaattori (IT)

Ryhmät 1 ja 2 koostuvat vain yhdestä, selkeästi muista eroteltavasta tekijästä. Näiden ryhmien painoarvo on kuitenkin suuri. Asiakas on luonnollisesti suuressa osassa, koska koko ohjelmistoprojekti käynnistyy asiakkaan tarpeista. Lisäksi asiakkaalla ei välttämättä ole kokemusta ja tietämystä ohjelmistoalasta, joten potentiaalisia riskitekijöitä on paljon.

Myynti on myös yrityksen kannalta haasteellinen osio, koska yrityksen tuotteita ja palveluita myyvät henkilöt eivät välttämättä tiedä miten ohjelmistoprojektit rakentuvat,

miten eri vaiheet vievät resursseja jne. Tällöin myyjä ei välttämättä osaa myydä asiakkaalle realistista kokonaisuutta (aika-resurssit-lopputulos, kohdassa 2.5 esitetty projektinhallintakolmio). Ryhmä kolme sisältää suoraan asiakaspalveluun liittyvät tahot, eli varsinaisen asiakaspalvelun, sekä hallinnollisesti asiakaspalvelun alle sijoittuvan Sovelluspalvelut-tiimin, joka saa ratkaistua suurimman osan asiakkaiden tukipyynnöistä.

Ryhmä 4 sisältää tuotehallintaan liittyvät tahot, eli tuotekehityksen, jonka alla tuote- ja projektipäälliköt toimivat. Tämä ryhmän alaiset vastaavat tuotteen kehittämiseen liittyen linjauksista, priorisoinneista ja muista toteuttavan tason työtä ja lopputuloksia ohjaavista asioista.

Ryhmä 5 koostuu tuotantotiimistä, tai -tiimeistä, sekä testaustiimistä. Ohjelmistoarkkitehdillä on joissain prosesseissa omat tehtävänsä, mutta ovat kuitenkin osa tuotantotiimiä. Ryhmässä 6 on Agenteqin prosesseissa ainoana erikseen mainittu tietovarasto, tukijärjestelmä. Sinne säilötään dokumentaatiot ja ratkaisut havaittuihin ja korjattuihin ongelmakohtiin. Tässä ryhmässä on myös Operaattori, joka tässä yhteydessä tarkoittaa käytännössä IT-tiimiä, joka asentaa päivitykset ja korjaukset asiakkaiden tuotantojärjestelmiin.

4.3 Riskin mittaamiskriteerit

4.3.1 Riskin vaikutusalueet

Ennen kuin riskejä aletaan kartoittamaan, pitää määrittää, millaisilla mittareilla riskejä käsitellään. OCTAVE Allegro –menetelmässä käytetään viittä eri vaikutusaluetta, joiden osalta jokaista riskiä arvioidaan. (Caralli 2007, s. 21,57) Niistä jokaisen alle on määritetty kolme eri tasoa, joista johonkin käsiteltävänä oleva riski sijoittuu (Matala-Keskiverto-Korkea).
Nämä OCTAVE Allegron viisi vaikutusaluetta ovat:

- Luotettavuus/Asiakastyytyväisyys
- Taloudellisuus
- Tuottavuus
- Turvallisuus ja terveys
- Sakot/laillisuuskysymykset

Näiden vaikutusalueiden osalta arviointi liittyy kohdassa 2.4.3 mainittuun kolmiportaiseen riskin vaikutuksen suuruuden arviointiin. Kohdassa 2.4.3 mainittiin McManusin (2004, s. 90) skaalaavan riskien vaikutukset kolmiportaiselle asteikolle. OCTAVE Allegron menetelmässä saadaan numeroarvo kuvaamaan riskin vaikutusta, mutta sen sijaan, että riskille annetaan vain yksi vaikutusarvot, muodostetaan tässä vaikutusarvo painottamalla eri osa-alueita. Kolmiportainen vaikutusarvo annetaan erikseen jokaiselle vaikutusalueelle. Mittaamiskriteerien määrittämiseen kuuluu näiden viiden vaikutusalueen järjestäminen prioriteetin mukaan. Alueille määritetään prioriteetit

1-5, jotka määräytyvät organisaation liiketoiminnallisten tavoitteiden perusteella. Vertaillaan kahta riskiä. Pääosin Luotettavuutta vahingoittavan riskin vaikutus on Matala ja vastaavasti eniten Taloudellisuuteen vaikuttavan riskin vaikutus on Korkea. Jos Luotettavuus on yrityksen riskinhallintastrategiassa priorisoitu merkittävimmäksi tekijäksi, ja Taloudellisuus vähiten merkittäväksi, päätyy Matalan vaikutuksen omaava riski lopullisessa prioriteettijärjestyksessä korkeammalle. Menetelmää havainnollistetaan kuvassa 4.2., joka on esimerkki OCTAVE Allegron omasta ohjeesta riskianalyysin tekoon.

Impact Area	Ranking	Impact Value	Score
Reputation	4	Moderate (2)	8
Financial	5	Low (1)	5
Productivity	3	Low (1)	3
Safety and Health	1	Low (1)	1
Fines/Legal	2	High (3)	6
		Total Score	**23**

Kuva 4.2. *Otos riskianalyysistä (Caralli 2007 s. 57)*

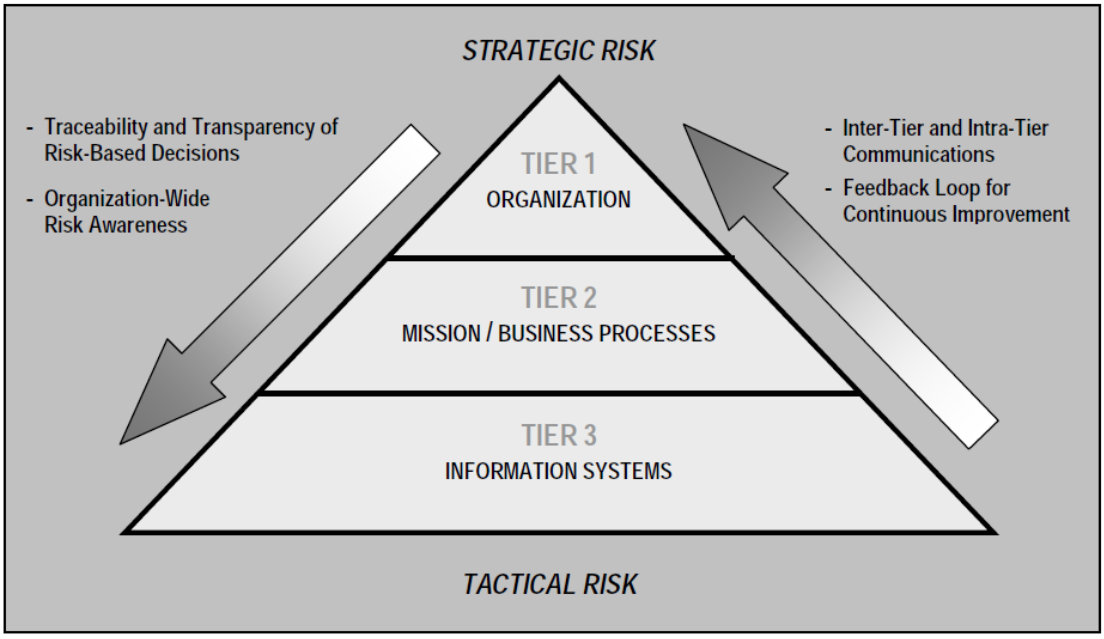
Nämä viisi kategoriaa kuvaavat nimenomaan riskin vaikutuksia liiketoiminnan osa-alueisiin, eivätkä riskien jaottelua erilaisiin kategorioihin, joita on lueteltu kohdassa 2.4.2. Molemmat jaottelutavat sopivat käytettäväksi rinnakkain. Kategoria- ja tyyppijaottelu helpottaa lievennystoimenpiteiden kohdentamista ja samankaltaisten riskien ”niputtamista” ja sitä kautta tehostaa riskinhallintaprosessia. OCTAVE Allegron jako ja priorisointi taas vaikuttaa konkreettisesti siihen, mitkä riskit päätyvät kriittisimmiksi ja sitä kautta korkeammalla prioriteetilla ratkaistavaksi.

Kuten riskinhallinnan menetelmät muutenkin, ovat nämä vaikutusalueet, sekä eri alueiden sisäisen vaikutusasteikon rajat yrityksen määriteltävissä. Nämä linjaukset tulisi tehdä riskinhallintaprosessin alussa, jotta riskien arviointi myöhemmin olisi helpompaa. Tällainen tarkka määrittäminen on haasteellista ja vaatii paljon resursseja (riittävän korkealta taholta, joka muutenkin on hyvin työllistetty). Esimerkkinä tällaisista rajoista voisi olla, että asiakkaan tekemä reklamaatio. Kuinka suuri reklamaation korvausvaatimuksen tulee olla, jotta ko. ongelman aiheuttava riski nousee Matala-luokituksesta Kohtuulliseen, tai jopa Korkeaan?

Kohdassa 2.4.3 on tuotu esiin riskin todennäköisyyden määrittäminen. Riskin todennäköisyyttä ja vakavuutta käytetään laskemaan riskin todellinen vaikutus. OCTAVE Allegron tapauksessa todennäköisyys on vapaaehtoista vaiheessa 5, jossa tunnistetaan resursseihin kohdistuvia uhkia. Allegron tapauksessa todennäköisyyksiä ei käytetä sellaisenaan konkreettisesti määritettäessä riskien kokonaisvaikutuksia tai keskinäisiä prioriteetteja, vaan laskenta tehdään kuvan 4.2. osoittamalla tavalla. Jos todennäköisyydet halutaan määrittää, tulee ne tehdä kaikkien arvioitavien resurssien kohdalla. Näitä todennäköisyyksiä voi riskien minimointivaiheessa käyttää ohjaavana tietona. Koska riskien todennäköisyyden tarkka määritteleminen voi olla todella vaikeaa, käytetään Allegrossa vain kolmiportaista asteikkoa, kuten riskin vaikutusasteikkokin. (Caralli 2007 s. 52)

4.3.2 Strateginen ja taktinen riskinhallinta

National Institute of Standards and Technology (tästä eteenpäin NIST) käy läpi riskien arviointia dokumentissaan Guide for Conducting Risk Assessments (NIST 2012). Dokumentti käsittelee riskinhallintaa pääpiirteittään samalla tavalla kuin on esitetty luvussa 2, mutta joitain sellaisia asioita tuodaan esiin, jotka ovat oleellisia juuri Agenteqin kannalta. Dokumentti sisältää riskien käsittelyä lähinnä tietoturvan kannalta, mutta mainitsee dokumentin esille tuoman kolmikerroksisen riskinhallintahierarkian soveltuvan myös Agenteqin prosessien tyyppisiin tapauksiin. Eli sen sijaan että käsiteltäisiin vain tietoturvaan liittyviä asioita, voidaan ottaa näkökulma kauempaa, yrityksen tuotannollisiin linjauksiin ja esimerkiksi tuotannon kehitystyökalujen hankintastrategiaan asti. Tämä pyramidimalli on esitetty kuvassa 4.3. Varsinkin pyramidin tasot 1 ja 2 ovat erittäin oleellisia Agenteqin prosesseissa, koska paljon ongelmakohtia kohdistuu hallinnolliseen tiedonkulkuun, muiden yrityksen tahojen tehokkuuden ja tietotarpeiden arviointiin, eikä vain varsinaiseen ohjelmiston suunnitteluun ja kirjoittamiseen.



Kuva 4.3. *Riskinhallintahierarkia (NIST 2012, s. 17)*

Ylintä tasoa, ja samalla strategista riskinhallintaa, ovat OCTAVE Allegron riskinhallintaprosessin alkupään vaiheet, jossa määritetään puitteet riskinhallinnalle. Lisäksi myös valittavat jaottelut riskikategorioista ja -tyypeistä ovat strategisia päätöksiä, jotka edesauttavat riskien painotusta, kohdentamista ja prioriteettia. Strateginen taso tarkoittaa esimerkiksi tapoja reagoida riskeihin, päätöksiä resurssien ohjaamisesta riskinhallintaan (ja tietoturvaan), hankinnoista päättämistä ja tietohallinnan linjauksia yrityksestä ulos ja sisään (asiakkaille ja asiakkailta) virtaavan tiedon suhteen. Taso 2 koskisi Agenteqin tapauksessa juuri tässä luvussa esitettyjä prosesseja, jotka ovat yrityksen itse määrittämiä, sekä myös menetelmät, joiden avulla näitä prosesseja tulevaisuudessa kehitetään. Lisäksi esimerkiksi kehitystyökalut ja palveluiden ylläpitoon tarvittavat ohjelmistot ja laitteistot ja niiden hankinnat kuuluvat tähän. Kolmannelle tasolle sijoittuvat prosessien aikana konkreettisesti tehtävät asiat, eli Agenteqin tapauksessa eri prosessien yksittäiset vaiheet, kohdassa 4.2 mainittujen ryhmien 3-6 osalta. Dokumentissa itsessäänkin tuodaan esiin nämä asiat, jotka pätevät tai ovat laajennettavissa tietoturvallisuuden ulkopuolelle. (NIST 2012, s. 17–18)

Tämä kolmikerroksinen malli sopii hyvin Agenteqin tilanteeseen, ja tukee sitä ajatusta, että saadakseen toteutettua kattava riskinhallinta koko yrityksen toiminnan laajuudelta (eli yksittäinen prosessi alusta loppuun kaikkien vaiheiden läpi), tarvitaan riskinhallintaorganisaatioon henkilöstöä suuresta osasta kohdassa 4.2 esitettyjä ryhmiä.

Vaikka Agenteqin prosessikaavioista saadaankin eriteltyä ”vastuutahot” ja niiden alle sijoittuvat eri tyyppisille ja erilaisille riskeille altistuvat toiminnot, ei tietyn toimijan vastuu kuitenkaan pääty kun prosessikaaviossa siirrytään viivan yli seuraavan toimijan alueelle. Esimerkiksi määrittelyvaiheessa realisoitunut riski informaatiokatkoksesta

asiakkaan kanssa voi aiheuttaa virheellisen määrittelyn päätymisen tuotantotiimille. Tällöin, vaikka tuotantotiimi tekisi työnsä täysin oikein, ja riskit olisivat hallinnassa, voi lopputulos olla silti ”virheellinen”. Tällöin tuhlatut resurssit voivat olla merkittäviä, koska realisoitunut riski on vaikuttanut toteutettavaan asiaan koko ajan.

Yrityksen tulee ottaa riskinhallintastrategian osaksi ohjeistus siitä, että miten tietyn kerroksen riskien arvioinnista saadaan tarvittava tieto jaettua muiden kerrosten riskien arvioitsijoille (NIST 2012, s. 22). Edellä mainitun jatkuvuusongelman takia täytyy pitää huoli riittävästä kommunikaatiosta eri riskinarvioitsijoiden välillä. Käytännön työssä kuitenkin aktiivinen viestittely on käynnissä asiakkaan, tuotehallinnan ja tuotantotiimin välillä, joten täysin taso kerrallaan eteneminen ei ole vaatimus onnistuneelle riskinhallinnalle.

NIST:n näkemys riskinhallintaan valmistautumisesta tukee hyvin OCTAVE Allegron vastaavaa, ja tuo erityisesti esiin muutamia asioita, jotka pätevät hyvin Agenteqin tilanteeseen. Aiemmin tässä luvussa esitettiin tapa priorisoida tietyn riskin vaikutusalueita, jolloin yrityksen toiminnan kannalta tärkeämpiin osa-alueisiin kohdistuvat riskit saavat enemmän huomiota kuin muut, vaikka muut sinänsä olisivatkin isoja riskejä omalla alueellaan. Tätä priorisointia sivuten NIST esittää arvioinnin alussa määritettäväksi arvioinnin laajuuden. Tällöin esimerkiksi yrityksen johto voi päättää suoraan jonkin osa-alueen poisjättämisen arvioinnin piiristä (NIST 2012, s. 25). Luonnollisena osana prosessia tämä voisi tulla kyseeseen esimerkiksi silloin, kun jotain kohdassa 4.1 esitettyä prosessia muutetaan merkittävästi. Kaikki prosessien osapuolet eivät välttämättä ole ko. prosessissa mukana, joten niiden osalta ei välttämättä ole tarpeen tehdä kattavaa riskien arviointia.

Riskiarvioinnin laajuuden määrittämiseen sisältyy myös aikaväli, jonka arvioinnin tulokset pystyvät validina (NIST 2012, s. 25). Prosessien pysyessä muuttumattomina varsinaiset prosessiin liittyvät riskit pysynevät ennallaan pitkänkin aikaa, mutta toisaalta erilaiset projektit eri asiakkaan, eri projektipäällikön ja eri tuotantotiimin välillä saattavat luoda epäsäännöllisyyttä, joka voi osaltaan olla syy riskiarvioiden tarkistamiseen useamminkin. Lisäksi riskiarvion tekeminen eri tasoilla kuvassa 4.3. esitettyä pyramidimallia saattaa vaatia eri määriä resursseja, joten sekin on otettava huomioon kriteerejä määritettäessä.

Vielä yksi huomioitava asia on riskiarvioinnin perusteena olevien tietolähteiden määrittäminen (NIST 2012, s. 27). Agenteqissa ei ole aikaisemmin tehty vastaavanlaista riskienhallintaa. Teemu Keiski käsitteli yrityksen tietoturvaa ja tietoturvariskejä lopputyössään (Keiski 2013), mutta riskejä Agenteqin prosessien suhteen ei ole aikaisemmin kartoitettu. Näin ollen ei ole olemassa valmista dataa tai suunnitelmaa siitä, miten riskinhallinta pitäisi aloittaa, tai millaisiin kokonaisuuksiin sitä olisi hyvä jakaa. Tätä ongelmaa onkin jo pohdittu, juuri pohjatietojen puuttumisen takia, kohdassa 4.2.

NIST:n mukaan oleellisen tiedon luonne vaihtelee riippuen siitä, millä tasolla kuvan 4.3. kuvaamassa mallissa ollaan. Ensimmäisellä tasolla tieto käsittelee esimerkiksi priorisointiin liittyvää tietoa. Toisella tasolla oleellinen tieto liittyy esimerkiksi prosessikaavioissa esitettyyn prosessin etenemiseen tai organisaation erillisten osien, ja myöskin tuotettavan palvelun erillisten osien väliseen kommunikointiin. Kolmannella tasolla tieto on esimerkiksi tietoa käytetyistä ohjelmistoarkkitehtuuriratkaisuista tai liittymistä muihin järjestelmiin. (NIST 2012, s. 27) Agenteqin tapauksessa monessa asiassa näiden kaikkiin kolmeen kerrokseen liittyvän tiedonkeräämisessä ja jakamisessa sitä tarvitseville tahoille on haasteita.

4.4 Resurssien kartoitus

OCTAVE Allegro –menetelmä on suunniteltu tietoturvariskien kartoitukseen, joten tämän diplomityön osalta sitä pitää soveltaa. Allegron vaiheessa 2 määritetään ne tietoresurssit, joissa ovat yrityksen kannalta oleellisia. Agenteqin tapauksessa suuri osa tiedosta ja tietämyksestä on sitoutuneena henkilöstöön, ja sen takia kaikkia tärkeitä tietoja ei saada katettua varsinaisten fyysisten resurssien kartoituksella. Avainhenkilöiden varassa olevan tiedon ja tietämyksen lisäksi on luonnollisesti olemassa fyysisiä tietovarastoja, palvelimia ja tietokantoja, joihin asiakkaiden ja yrityksen omat tiedot ovat tallennettuina. Allegron vaiheessa 3 selvitetään ja avataan tietovarastot, joihin edellä mainittu tieto on varastoitunut. Agenteqin tapauksessa nämä pitävät sisällään henkilöstön, työasemat, palvelimet ja tietokannat.

Agenteqin riskinhallinnassa tässä vaiheessa varsinaisiin tietovarastoihin kannattaa rinnastaa kohdassa 4.2 esitetyt ryhmät ja niiden sisältämät osapuolet. Myöhemmin riskinhallintaprosessissa kartoitetaan jokaista tällaista tietovarastoa koskevat potentiaaliset ongelma-alueet, sekä näiden ongelmakohtien kautta uhkaavat tilanteet. Tämä kartoitus tehdään siis koskemaan myös kohdan 4.2 ryhmiä. Esimerkiksi ryhmässä 4 voisi olla vaarana tietyn asiakasprojektin tärkeiden tietojen oleminen vain yhden henkilön tiedossa dokumentoimattomana. Vastaava uhka varsinaisen tietovaraston osalta voisi olla esimerkiksi varmuuskopioinnin puuttuminen.

4.5 Uhkien tunnistaminen

OCTAVE Allegrossa uhkien tunnistaminen koostuu ongelmakohtien etsimisestä (Allegron vaihe 4), ja niiden perusteella tehtävien uhkaskenaarioiden määrittämisestä (Allegron vaihe 5). Nämä vaiheet 4 ja 5 ovat käytännössä kohdassa 2.4 esitellyn

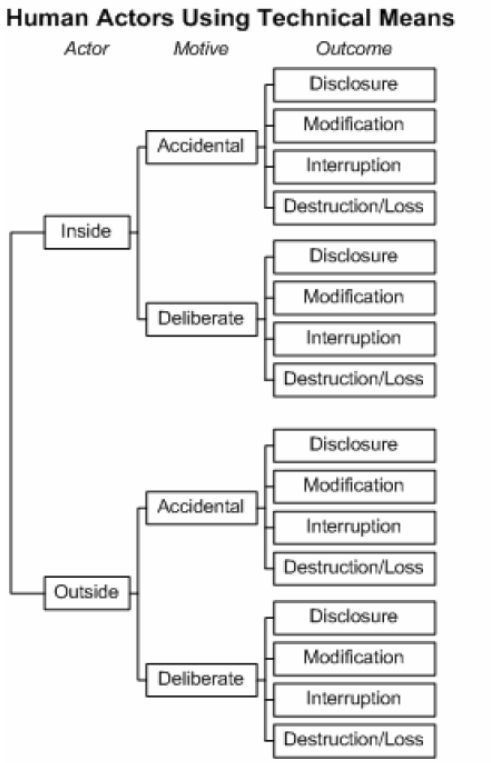
riskinhallintaprosessin vaiheet 1 ja 2. Kun riskien selvittäminen aloitetaan näin uhkien kautta avaamalla, on kyseessä uhkasuuntautunut lähestymistapa. (NIST 2012, s. 15)

Uhkia tunnistettaessa suuressa arvossa ovat riskinhallintaorganisaation jäsenten henkilökohtaiset tiedot ja kokemukset. Aiempien onnistumisten, epäonnistumisten ja läheltä piti -tilanteiden perusteella jokaiselle on muodostunut kuva oman osaamis- ja vastuualueensa heikkouksista ja ongelmakohdista. Tämä on jälleen konkreettinen tilanne, jossa käytännössä tulee ilmi tarve yksinkertaistetulle jaolle henkilöstön jäsenten välillä, kuten kohdassa 4.2 on tehty. Omien kokemusten ja tietämyksen lisäksi voidaan suuntaa-antavana ohjeena käyttää resurssien kartoittamisen yhteydessä tuotettua tietoa, josta tulisi käydä ilmi prosessikohtaisesti resurssiin liittyvät muut tahot.

Ongelmakohtien tunnistamisen jälkeen niiden perusteella kartoitetaan varsinaiset uhat, joista riskit muodostuvat. Riskinhallinnan tapauksessa uhkakuvaus pitää sisällään seuraavat tiedot (Caralli 2007, s. 48):

- resurssi – jotain, josta on yritykselle arvoa
- keino – kuinka jokin taho/tapahtuma voi päästä resurssiin käsiksi
- tekijä – kuka tai mikä käsittelee resurssia
- motiivi – pätee vain ihmisiin, miksi joku haluaa aiheuttaa haittaa resurssille
- lopputulos – välitön seuraus, joka uhan toteutumisesta resurssille aiheutuu

Tiedoissa näkyy menetelmän tietoturvapainotteisuus. Keino, tekijä ja motiivi koskevat juurikin tietovarastossa olevaa tietoa, ja eivät liity henkilöön tai henkilön toimiin. Agenteqin tapauksessa tietovarastojen lisäksi resursseina toimivat henkilöt ja heidän tekonsa. Täten kaikkien uhkien kohdalla ei kaikkia tietoja ole, ja uhkia listatessa kyseessä oleva tieto jää tyhjäksi. Uhkien määrittämisen apuna voi käyttää OCTAVO Allegron Uhkapuita (Threat Tree), joissa on puumaiseen rakenteeseen jaoteltu erilaisia uhkatyyppejä. Esimerkkinä olevat uhkapuut sopivat parhaiten tietoturvauhkiin. Nämä uhkapuut on esitetty liitteessä 1. Kuvassa 4.9. on esimerkinomaisesti esitetty yksi puista, ihmistoimijat käyttäen teknisiä keinoja.



Kuva 4.4. *Otos liitteestä 1. Uhkapuu, ihmistekijä teknisin keinoin (Caralli 2007, s. 50)*

Kun ongelmakohdat ja niihin mahdollisesti kohdistuvat uhat on selvitetty, sekä edellä mainitut tiedot uhille on selvitetty, voidaan siirtyä varsinaisten riskien arviointiin. Listatut uhat tulee kuitenkin käydä läpi, ja jos ollaan sitä mieltä, että uhka ei realistisesti voi ikinä toteutua, voidaan se jättää pois myöhemmistä käsittelyistä.

4.6 Riskien tunnistaminen ja lievennys

4.6.1 Riskien tunnistaminen ja analysointi

Edellisen vaiheen seurauksena on selvitetty resursseja koskevat uhat (niiltä osin kun ne sisältyvät kohdan 4.3 mukaisesti määritettyyn suoritettavaan riskiarviointiin). Varsinainen riski muodostuu edellä mainitusta uhasta, ja uhan realisoituessa resurssille aiheutuvasta seurauksesta (Caralli 2007, s. 53). Jokaisella määritetyllä uhalla tulee toteutuessaan olla jokin organisaatiolle vahingollinen seuraus. Seurausten kartoittamisen tulisi olla riskinhallintaorganisaatiolle selkeää, koska tällä eri tasoilta organisaatiosta räätälöidyllä henkilöstöllä pitäisi olla riittävästi tietoa kaikkien mahdollisten seurausten selvittämiseen. Ongelmaksi saattaa muodostua tiedostettujen kerrannaisvaikutusten dokumentointi.

Kohdassa 4.1 läpikäydyt prosessit kuvaavat yksittäisiä, tietyntyyppisiä prosesseja, eikä samanaikaisesti käynnissä olevien saman tyyppisten tai erilaisten prosessien suhteita toisiinsa ole otettu huomioon. Tällöin toteutuneen uhan seuraukset eivät välttämättä

rajoitu esimerkiksi kyseisen prosessin seuraavan vaiheen viivästymiseen, vaan mahdollisesti tuotantotiimin meneillään olevan sprintin toteutuminen voi vaarantua. OCTAVE Allegro -riskinhallintamenetelmän ohjeessa esimerkki seurausten määrittämisestä on huomattavasti suoraviivaisempi: työntekijä pääsee vahingossa näkemään kollegansa henkilökohtaisia tietoja, ja seurauksena on sakkoja yritykselle (Carelli 2007, s. 54). Agenteqin tapauksessa tämä rinnastuu kyseisen prosessin sisäiseen etenemiseen liittyviin seurauksiin, mutta lisäksi uhan toteutuessa saatetaan vaatia tuotehallinnalta resursseja tulevien työtehtävin aikataulujen ja prioriteettien muutoksiin.

Seurausten määrittämisen myötä tuloksena on lista riskeistä, jotka käynnissä olevan riskiarvioinnin puitteissa käydään läpi. Kohdassa 4.3 määritettiin yrityksessä riskin mittaamiskriteerit, eli erityyppisten seurausten vakavuusasteikot. Lisäksi annettiin vaikutusalueille painoarvot. Jos riskeille määritetyt seuraukset ovat tarkkaan mietityt, ja mittaamiskriteerien yhteydessä on panostettu yrityksen toimintaa ja prioriteetteja kuvaavan asteikon luomiseen, pitäisi riskien läpikäynti olla varsin suoraviivaista. Kohdassa 4.3 mainittiin uhkien todennäköisyyksien olevan vapaaehtoisia. Jos ne on päätetty ottaa mukaan erillisinä, pidetään niitä mukana vielä lievennysvaiheeseen asti. Muuten, lievennysvaihtoehtoa valittaessa todennäköisyyttä pitää vielä erikseen arvioida.

4.6.2 Riskien lievennys

OCTAVE Allegro määrittää riskeille kolme mahdollista lähestymistapaa: hyväksyminen, lievennys ja lykkääminen. Riski voidaan hyväksyä, jos sen vaikutus on niin pieni, että sen mahdolliset seuraukset hyväksytään. Riskin lykkääminen tarkoittaa sitä, että riski jätetään odottamaan lisätietoja tai lisäselvitystä, ja siihen palataan myöhemmin. Jotta riskin lieventämistä voidaan lykätä, se ei voi olla vaikutuksiltaan kovin vakava. Lievennettävät riskit ovat sellaisia riskejä, joilla toteutuessaan olisi konkreettinen huono vaikutus näkökulmasta riippuen projektiin, prosessiin tai jopa yritykseen. Näille riskeille on etsittävä keinot vähentää niiden aiheuttamaa vaikutusta.

Kun jokainen riski on käyty läpi, ja niille päätetty jokin edellä mainitusta kolmesta vaihtoehdosta, on silti mahdollista, että jää vielä riskejä. Näitä riskejä kutsutaan jäänneriskeiksi. Esimerkiksi jokin riski voidaan lievennystoimenpiteillä saada hyväksyttävämmäksi, mutta riskiä ei kokonaan saada poistettua. Kyseinen riski jää siten jäänneriskiksi. Toimenpiteitä tulee kuitenkin saada tehtyä niin pitkälle, että jäänneriskitkin voidaan hyväksyä. (Caralli 2007, s. 58)

Käsiteltävät riskit tulee priorisoida. Tähän antaa suuntaa mahdollinen riskin realisoitumisen todennäköisyys, sekä riskin analysoinnissa määritetyt pistemäärät. Koska vaikutusalueiden, niiden painoarvojen ja epätarkkojen asteikoiden takia pistemääriin ei voi sokeasti luottaa, on riskinhallinnasta vastaavan henkilön tai yrityksen johdon on tuotava näkemyksensä asiasta esiin. Kaikkien lievennettäväksi päätyvien riskien kohdalla tulee suunnitella strategia, jolla riski saadaan pienennettyä sellaiseksi, että se voidaan

hyväksyä. Tämä vaihe on oleellisin koko riskinhallintaprosessissa. Aiemmat vaiheet ovat olleet varsin suoraviivaisia, ja vaatimuksina on ollut lähinnä vain riittävän tietämyksen omaaminen käsiteltävästä alueesta (Agenteqin tapauksessa prosessien tietyistä vaiheista). Lievennysstrategioista ja –toimenpiteistä päätettäessä saatetaan joutua tekemään merkittäviäkin taktisia tai strategisia muutoksia toimintatapoihin ja käytäntöihin. Muutosten hyväksyntä luonnollisesti täytyy tehdä korkeammalla tasolla, eikä vain riskinhallintaorganisaation sisällä.

Tässä vaiheessa luodaan uusia tai käytetään olemassa olevia riskin lievennysstrategioita, joiden taustateoriaa on esitetty kohdassa 2.4.5. Ensimmäisellä kerralla, kun yrityksessä tehdään riskinhallintaa, vienee tämä vaihe paljon resursseja. Tavoitteena tulisikin olla sellaisten strategioiden luominen, jotta niitä voidaan käyttää mahdollisimman laajasti tulevissa riskinhallintaiteraatioissa. Lievennystoimenpiteissä on tärkeää muistaa, että lieventämisen takia tehtävien muutosten, esimerkiksi aikataulun venyttämisen tai lopputuloksen laadusta tinkimisen, tulee olla järkevässä suhteessa realisoituvan riskin aiheuttaman haitan kanssa (Caralli 2007, s. 60). Luonnollisesti lievennysstrategioiden tulisi itsessään pyrkiä ohjaamaan toimintatapoja riskittömämpään suuntaan, joten tavoitteena ei tule olla vain uudelleenkäytettävyys tulevaisuudessa.

Kohdan 2.4.5 lieventämisstrategioista lähinnä riskin pienennysstrategiat ja jäänneriskistrategiat sopivat riskinhallintaprosessin tähän vaiheeseen. Nämä kaksi liittyvät juuri käsillä olevan riskin pienentämiseen vähintään hyväksyttävälle tasolle. Riskien välttämisstrategiat pyrkivät estämään riskien syntymistä. Agenteqin näkökulmasta olisi hyvä, jos riskinhallinnan kautta saataisiin kartoitettua mahdolliset suuremman mittakaavan ongelmakohdat, ja tulevaisuudessa kerätyn tiedon ja tietämyksen avulla pystyttäisiin riskejä välttämään esimerkiksi kohdan 4.1 prosessien sisältöä muokkaamalla. Siirtostrategioiden avulla voitaisiin löytää tapoja ohjata kiireisiltä henkilöiltä riskien pienentämiseen liittyviä tehtäviä toiselle taholle, mutta se vaatisi myös ylemmän tason muutoksia prosesseihin. Agenteqissa työtehtävät ovat jakautuneet varsin kiinteästi, johon kohdan 4.2 ryhmäjakokin perustuu. Tästä syystä, jos ajatellaan riskien kohdistuvan pääsääntöisesti prosessikaavioissa esitettyihin toimenpiteisiin, ei riskien siirtäminen muille osapuolille ole nykymallissa välttämättä kovin tehokasta. Tämä tarkoittaa sitä, että kun riskinhallinta on saatu osaksi rutiininomaista toimintaa, tulee keskittyä nimenomaan riskien välttämiseen, jotta näitä ongelmakohtia ei edes uhkia kartoittaessa tule esiin.

Kohdassa 2.5 esiteltiin projektinhallintakolmio, joka kuvaa projektin hallintaa kolmen suuren, toisistaan riippuvan osa-alueen välillä. Kun riskinhallintaa on suoritettu, ja mahdollisesti luotu strategioita riskien välttämiseksi ja lieventämiseksi tulevaisuudessa, voidaan tuloksia tarkastella projektinhallintakolmion näkökulmasta. Riskinhallinnan tavoitteena on vähentää tarvetta projektinhallintakolmiossa tehtäviin äkillisiin

muutoksiin, jossa esimerkiksi aikarajan lähestyessä täytyykin hankkia merkittävästi lisäresursseja laadukkaan tuotteen valmiiksi saamiseksi.

Osan riskin aiheuttavista uhista saa poistettua, mutta koska kaikkien uhkien kohdalla se ei onnistu, on osa käytettävistä strategioista sellaisia, joilla minimoidaan potentiaaliset vahingot. Näitä ovat välttämisstrategiat ja lievennysstrategiat. Näissä toimenpiteet voivat hyvinkin olla käytännössä projektinhallintakolmion painopisteiden säätämistä. Hallitusti ja hyvissä ajoin tapahtuvat muutokset ovat huomattavasti parempia kuin kiireessä tehdyt hätäratkaisut. Ja vaikka ei tietenkään ole periaatteessa hyvä asia, että asiakasta joudutaan informoimaan työn viivästymisestä tai joudutaan ottamaan käyttöön lisäresursseja työn kannattavuuden kustannuksella, ovat ne sellaisia myönnytyksiä, joita joka tapauksessa joudutaan tekemään riskinhallinnassa. On kuitenkin pidettävä mielessä se tärkeä asia, että riskin lievennyksestä koituvan haitan tulee olla järkevässä suhteessa riskistä aiheutuvaan haittaan.

4.7 Riskinhallintaesimerkki

Käydään läpi yhden prosessin riskinhallintaa. Käytetään esimerkkinä kohdassa 4.1.6 ja liitteessä 6 esiteltyä bugi- ja hotfix-prosessia. Tämän diplomityön puitteissa ei suoriteta kattavaa riskinhallintatoimintaa, vaan käydään esimerkinomaisesti vaihe vaiheelta läpi, miten prosessi tulisi oikeasti liiketoiminnassa etenemään. Käsitellään myös riskinhallintaprosessin aloittamistoimenpiteitä, kuten riskinhallintaorganisaation ja riskitietokannan muodostamista.

4.7.1 Riskinhallintaorganisaatio

Bugi- ja hotfix-prosessiin ovat osallisena kohdassa 4.2 määritetyistä ryhmistä ryhmät 1, 3, 4, 5 ja 6. Jokaisesta näistä ryhmästä pitäisi mukana olla vähintään yksi henkilöstön jäsen. Lisäksi yhden ryhmän jäsenen tulisi olla joko itse sellaisessa asemassa, jossa hän voi tehdä linjauksia resursointiin ja strategisia muutoksia, tai olla muuten yhteydessä yrityksen ylempään johtoon. Jälkimmäisessä tapauksessa esille tulleet riskinhallinnalliset asiat saadaan käsiteltyä johdon kanssa esimerkiksi viikoittaisissa palavereissa muiden tehtävien ohessa.

Tässä prosessissa asiakkaan rooli on pieni, ja kaksisuuntaista kommunikaatiota asiakkaan kanssa ei tapahdu. Näin ollen asiakasosapuolta ei tarvitse huomioida riskinhallintaorganisaatiossa. Riskinhallintaorganisaatio koostuu siis neljästä henkilöstä, joista ryhmään 4 (tuotekehitys, projekti- ja tuotepäälliköt) kuuluva henkilö on esimiesasemassa ja omaa valtaa tuotannon linjauksista päättämiseen. Tuotekehityksellä ei ole tässä prosessissa konkreettisia tehtäviä, koska sen kohdalla prosessia käynnistyy

tuotekehitysprosessi. Tuotekehitysprosessin riskinhallinta tehdään erillään nyt käsiteltävänä olevasta prosessista.

4.7.2 Mittaamiskriteerit

Mittaamiskriteerien määrittäminen kokonaisuudessaan riskinhallintaorganisaation sisällä on mahdotonta, sillä niihin vaikuttavat mahdollisesti yrityksen johtoryhmän näkemykset. Työntekijöille kuitenkin tuodaan esiin yrityksen tavoitteita ja toiminnan painopisteitä, joten jonkinlaisen priorisoinnin riskien välillä he voivat tehdä. Varsinaiset riskinhallinnan strategiset linjaukset tulee kuitenkin hyväksyttää ylempää.

Tässä esimerkkitapauksessa jätetään vähemmälle prioriteetille kohdan 4.3 vaikutusalueista sakot/laillisuuskysymykset sekä turvallisuus ja terveys. Laillisuusasioiden ohittaminen selittyy sillä, että tuotannon työntekijöillä ei ole tietämystä niiden luotettavaan käsittelyyn. Turvallisuus ja terveys jätetään vähemmälle tärkeydelle siksi, että toimistotyössä pääosin päätetyöskentelyssä ovat työtapaturmat ja ulkoiset uhat terveydelle vähäisiä.

Agenteqin liiketoiminnassa asiakastyytyväisyys on merkittävässä osassa. Lisäksi, koska kyseessä on kuitenkin yritystoiminta, on myös tuottavuus tärkeää. Asetetaan siis OCTAVE Allegron mukaisten vaikutusalueiden keskinäinen priorisointi ja painoarvot seuraavasti: Luotettavuus/asiakastyytyväisyys(5), Tuottavuus(4), Taloudellisuus(3), Turvallisuus ja terveys(2) ja Sakot/laillisuuskysymykset(1). Näitä painotuksia käytetään riskien analysointivaiheessa.

Riskityyppien käyttö helpottaa myöhemmässä vaiheessa uhkien ja riskien kartoittamista. Tarkasteltavia resursseja voidaan käydä läpi riskityyppi kerrallaan, jolloin on helpompi keskittyä kapeampaan alueeseen kerrallaan. Riskityypit voivat muotoutua ajan kuluessa vastaamaan yrityksen tarpeita, mutta käytetään tässä kohdassa 2.4.2 esiteltyä kuuden riskityypin jaottelua. Riskityypit ovat teknologiariskit, henkilöriskit, organisaatioriskit, työkaluriskit, vaatimusriskit ja arviointiriskit.

4.7.3 Riskitietokanta

Tulevaisuuden ja oppimisen takia pitää perustaa jonkinlainen riskitietokanta, johon säilötään riskeihin ja niiden käsittelyyn liittyvät oleelliset tiedot. Kattavan riskinhallinnan ja sujuvan toiminnan mahdollistamiseksi tullaan todennäköisesti tarvitsemaan sisäinen kehitysprojekti, jotta saadaan toteutettua tehokas työkalu riskitiedon hallintaan.

Agenteqin nykyisillä tietojärjestelmätyökaluilla saataisiin ylläpidettyä wiki-tyyppisesti riskeihin liittyviä riskinhallintastrategioita. Tämä saattaa olla riittävä sellaisissa

tapauksissa, joissa löydettyjen riskien kautta päädytään muuttamaan toimintaa prosessitasolla. Merkittävät muutostarpeet olisivat saatavilla helposti, ja niitä olisi varsin helppoa työstää eteenpäin. Ajan kuluessa ja riskinhallinnan laajentuessa jopa koko yrityksen toimintaan, kasvaa tietomäärä liian suureksi wiki-periaatteella toimivalle järjestelmälle. Kun tietyn prosessin uhkia ja riskejä kartoitetaan, tulee pääsyn vastaavien riskien historiatietoon ja lievennysstrategioihin olla nopeaa ja sujuvaa. Tästä syystä tarvittaisiin erillinen käyttöliittymä mahdollisine koostettavine raportteineen riskien käsittelyyn.

Järjestelmän suunnittelu ja toteuttaminen tulee olemaan oma projektinsa, joten aluksi käytetään yksinkertaista tietokantarakennetta. Tietokantaan tallennetaan riskien jaotteluissa käytetyt kategoriat ja tyypit. Lisäksi pitää tallentaa jonkinlainen kuvaus riskeiltä varjeltavista resursseista, uhista ja riskeistä. Myös historiatieto pitää pystyä säilyttämään, esimerkiksi muuttuneiden riskityyppien osalta.

Riskitietokannan tulee sisältää ainakin seuraavat tiedot:

- Riskityypit, -kategoriat ja vaikutusalueet
- Resurssit prosessikohtaisesti
- Uhat resurssikohtaisesti
    - Resurssi, johon uhka kohdistuu
    - Kuvaus resurssin haavoittuvuudesta
    - Uhan aiheuttaja
    - Mahdolliset seuraukset
- Uhkiin ja resursseihin liittyvät riskit
    - Uhka, johon riski liittyy
    - Riskin vakavuus
    - Riskin todennäköisyys
    - Riskiin liittyvät lieventämisstrategiat
    - Riskin nykytilanne ja mahdolliset tehdyt toimenpiteet
- Lieventämisstrategiat tyypeittäin
    - Millaisia strategioita erilaisiin riskeihin on kohdennettu

4.7.4 Resurssien kartoitus

Riskinhallintaa lähestytään prosessikohtaisesti. Kohdassa 4.2 ryhmiteltiin prosesseissa mukana olevia osapuolia. Resurssien kartoittamisessa puretaan prosessi ja sen osapuolet auki, jolloin saadaan lista osapuolten työvaiheista. Listataan prosessin osapuolet, sekä avataan auki listaksi prosessikaavion (liite 6) vaiheet.

- Asiakas
    - Saa tiedon tehdystä korjauksesta
- Asiakaspalvelu
    - Saa sovelluspalveluilta tiedon, että korjaus on tehty
    - Tiedottaa asiakasta korjauksesta

- Sovelluspalvelu
    - Havaitsee bugin
    - Määrittelee bugin kriittisyyden
    - Kirjaa bugin järjestelmään ja aktivoi sen kehitystiimin työlistalle
    - Luo päivityssuunnitelman asiakkaan järjestelmään korjauksen valmistuttua
    - Jakaa viimeistelytehtävät asiakaspalvelun, sovelluspalvelun, kehitystiimin ja operaattorin välillä
    - Testaa ominaisuuden toiminnan asennuksen jälkeen
- Kehitystiimi
    - Saa sovelluspalveluilta tiedon bugista
    - Ottaa bugikorjauksen työn alle työjärjestyksen mukaisesti
    - Korjaa ja testaa bugikorjauksen
    - Luo päivityspaketin valmiiksi odottamaan asiakkaan järjestelmään asennusta
    - Välittää tiedon korjauksen valmistumisesta sovelluspalveluille
    - Tarvittaessa avustaa testaamisessa asennuksen jälkeen
- Operaattori
    - Asentaa korjauspäivityksen asiakkaan järjestelmään

Tuloksena saatiin viiden eri toimijan alle lueteltuna 16 kohtaa, joiden osalta riskejä lähdetään kartoittamaan.

4.7.5 Uhkien tunnistaminen

Seuraavaksi käydään läpi edellisessä kohdassa listatut 16 prosessin vaihetta, ja selvitetään niihin kohdistuvat uhat. Uhat kirjataan riskitietokantaan oheistietoineen. Riskinhallintaorganisaatio käy ryhmänä läpi vaiheet, ja yhdessä pyrkii tietämystään hyödyntäen selvittämään uhat mahdollisimman kattavasti.

Käydään esimerkinomaisesti läpi ensin Asiakaspalveluun kohdistuvien uhkien kartoitusta. Käytetään apuna riskityyppejä, jotta saadaan katettua erityyppisiksi riskeiksi muodostuvat uhat. Tässä esimerkissä ei ole tarkoitus löytää kaikkia mahdollisia uhkia, vaan havainnollistaa vaiheiden ja riskityyppien läpikäynti. Kohdassa 4.5 on mainittu Carallin (2007, s. 48) mainitsemat tiedot, jotka uhkakuvaukseen tulee sisällyttää. Listasta huomaa, että OCTAVE Allegro on suunniteltu tietoturvariskien näkökulmasta, koska mukana ovat keino, tekijä ja motiivi. Agenteqin tapauksessa uhat kohdistuvat usein henkilöihin ja heidän toimiinsa, eivätkä niinkään tietoihin. Tästä syystä nyt on jätetty riskinhallintaprosessin yksinkertaistamiseksi edellä mainitut kolme tietoa pois.

Resurssi 1: Saa sovelluspalveluilta tiedon, että korjaus on tehty

- Teknologiariskit

    - Uhka 1a: Yrityksen tietojärjestelmässä on käyttökatkos, joten tieto ei kulkeudu asiakaspalvelulle. Seuraus: Asiakastyytyväisyys kärsii, kun asiakas joutuu odottamaan jo valmistunutta korjausta.
- Henkilöriskit
    - Uhka 1b: Työntekijä ottaa työtehtävän omiin nimiinsä, mutta ei ehdi saamaan sitä valmiiksi, ja on seuraavana päivänä estynyt tulemaan töihin. Seuraus: Asiakastyytyväisyys kärsii, kun asiakas joutuu odottamaan jo valmistunutta korjausta.
- Organisaatioriskit
    - Uhka 1c: Yritys lisää resursseja kehitystiimiin, jolloin korjauksia valmistuu nopeammin kuin asiakaspalvelu ehtii informoimaan asiakasta. Seuraus: Yritys ei toimi niin tehokkaasti kuin olisi mahdollista.
- Työkaluriskit
    - Uhka 1e: Yrityksellä ei ole vapaana käyttöoikeuslisenssejä tarvittaviin ohjelmistoihin, joten uusi työntekijä ei pääse aloittamaan töitään. Seuraus: Yritys ei toimi niin tehokkaasti kuin olisi mahdollista.
- Vaatimusriskit
    - Uhka 1f: Yritys linjaa yllättäen, että asiakkaalle on saatava tieto lyhemmässä ajassa kuin aikaisemmin. Seuraus: Henkilöstön resurssit eivät välttämättä riitä täyttämään vaatimuksia.
- Arviointiriskit
    - Uhka 1g: Liian pieni osa asiakaspalveluhenkilöstössä on resursoitu juuri tämän vaiheen suorittamiseen. Seuraus: Yritys ei toimi niin tehokkaasti kuin olisi mahdollista.

Resurssi 2: Tiedottaa asiakasta korjauksesta

- Teknologiariskit
    - Uhka 2a: Yhteys sähköpostipalvelimeen katkeaa, ja sähköpostia ei voida lähettää. Seuraus: Asiakastyytyväisyys kärsii, kun asiakas joutuu odottamaan jo valmistunutta korjausta.
    - Uhka 2b: Sisäisessä tietoverkossa on toimintahäiriö, eikä asiakkaan yhteystietoja saada selvitettyä. Seuraus: Asiakastyytyväisyys kärsii, kun asiakas joutuu odottamaan jo valmistunutta korjausta.
- Henkilöriskit
    - Uhka 2c: Influenssakaudella jopa kolmannes asiakaspalvelun henkilöstöstä on sairaslomalla, joten asiakkaita ei ehditä informoimaan tarpeeksi nopeasti. Seuraus: Asiakastyytyväisyys kärsii, kun asiakas joutuu odottamaan jo valmistunutta korjausta.
- Organisaatioriskit
    - Uhka 2d: Asiakaspalvelulla on koulutuspäivä, jolloin kiireistä asiaa ei saada viestittyä asiakkaalle. Seuraus: Asiakastyytyväisyys kärsii, kun asiakas joutuu odottamaan jo valmistunutta korjausta.
- Työkaluriskit

    - Uhka 2e: Puhelinoperaattorin verkko on alhaalla, joten asiakkaalle ei voida soittaa. Seuraus: Asiakastyytyväisyys kärsii, kun asiakas joutuu odottamaan jo valmistunutta korjausta.
- Vaatimusriskit
    - Uhka 2f: Asiakas muuttaa toimintatapojaan, ja on vaikeampi tavoittaa. Asiakaspalvelulta menee turhien yhteydenottoyritysten takia resursseja hukkaan. Seuraus: Yritys ei toimi niin tehokkaasti kuin olisi mahdollista.
- Arviointiriskit
    - Uhka 2g: Uuden työntekijän perehdyttämisessä ei oteta huomioon aukkoja toimialatietämyksessä. Seuraus: Tarvitaan enemmän kommunikointia asiakkaan kanssa tai yrityksen sisäisesti, jolloin tehokkuus laskee.

Uhkalistaa tarkastelemalla huomataan, että moni uhka sopisi myös toisen resurssikohdan alle tai toisen riskityypin alle. Tämän on täysin luonnollista, eikä siitä ole haittaa. Tavoite on kuitenkin vain saada kaikki uhat käytyä läpi. Esimerkkiuhista nähdään, että asiakaspalvelun ollessa kyseessä, uhkien vaikutukset kohdistuvat lähinnä asiakastyytyväisyyteen ja yrityksen toiminnan tehokkuuteen.

4.7.6 Riskien tunnistaminen ja analysointi

Uhasta ja seurauksesta muodostuvat riskit tulee priorisoida. Kohdassa 4.3 on esitetty OCTAVE Allegron priorisointitapa, jossa painotetaan riskin eri vaikutusalueita. Tämä menetelmä saattaa hyvinkin osoittautua tulevaisuudessa liian pikkutarkaksi, koska eri vaikutusalueisiin kohdistuvien vaikutusten määrittäminen muuten suhteellisen matalan prioriteetin riskien kohdalla ei ole tehokasta. Nyt kuitenkin käydään esimerkkinä läpi uhat 1a ja 2f ja niiden priorisoinnit.

Uhka 1a, ”Yrityksen tietojärjestelmässä on käyttökatkos, joten tieto ei kulkeudu asiakaspalvelulle” kohdistuu asiakastyytyväisyyteen. Yksittäinen myöhästyminen ei kuitenkaan ole kovin vakavaa, vaan merkittävästi asiakastyytyväisyys alkaa laskea vasta riskin uusiutuessa. Kuvassa 4.5. on esitetty uhasta 1a syntyneen riskin vaikutusarvon muodostuminen.

Vaikutusalue	Sijoitus	Vaikutus	Pisteet
Luotettavuus/ Asiakastyytyväisyys	5	Kohtuullinen(2)	10
Taloudellisuus	3	Kohtuullinen(2)	6
Tuottavuus	4	Matala(1)	4
Turvallisuus ja terveys	2	Matala(1)	2
Sakot/ laillisuuskysymykset	1	Matala(1)	1
		Yhteensä	23

Kuva 4.5. *Riskin 1a priorisoinnissa käytetyn arvon muodostuminen*

Uhka 2f, ”Asiakas muuttaa toimintatapojaan, ja on vaikeampi tavoittaa.”. Tämäkään uhka ei aiheuta toteutuessaan merkittäviä vaikutuksia. Negatiiviset vaikutukset eivät kuitenkaan kohdistu asiakastyytyväisyyteen kuten uhan 1a kohdalla, vaan enemmänkin yrityksen sisäiseen tehokkuuteen. Tähän uhan vaikutusarvon muodostuminen on esitetty kuvassa 4.6.

Vaikutusalue	Sijoitus	Vaikutus	Pisteet
Luotettavuus/ Asiakastyytyväisyys	5	Matala(1)	5
Taloudellisuus	3	Kohtuullinen(2)	6
Tuottavuus	4	Kohtuullinen(2)	8
Turvallisuus ja terveys	2	Matala(1)	2
Sakot/ laillisuuskysymykset	1	Matala(1)	1
		Yhteensä	22

Kuva 4.6. *Riskin 2f priorisoinnissa käytetyn arvon muodostuminen*

Kuvista huomataan, että tätä arvoitusmenetelmää käyttäen 1a:han perustuva riski on kriittisempi kuin 2f. Kun vastaava (tai yksinkertaistettu) priorisointi on tehty kaikille riskeille, voidaan riskit järjestää pistemäärän mukaan prioriteettijärjestykseen. Riskien lieventämistä tulee aloittaa suunnittelemaan tässä järjestyksessä.

Riskien keskinäisen priorisoinnin lisäksi yksinkertaisemmin kuvatut uhkien seuraukset tulee riskien kohdalla avata tarkemmin. Näiden kahden esimerkkiriskin kohdalla seuraukset ovat pääpiirteittään selkeät, mutta lievennystoimenpiteitä voi olla vaikea kohdistaa oikein. Esimerkiksi riskin 2f tapauksessa voitaisiin määrittää, missä vaiheessa

tuhlattujen resurssien kustannus ylittää kriittisen pisteen. Tällöin osataan lievennystoimenpiteissä ottaa sopivan voimakkaat keinot käyttöön.

4.7.7 Riskien lievennys

Kohdan 4.6.2 mukaisesti tässä vaiheessa riskit joko hyväksytään, lykätään tai lievennetään. Otetaan esimerkeiksi edellisessä kohdassa malliksi käsitellyt riskit (käytetään kohdan 4.7.5 uhkalistasta tuttuja termejä 1a ja 2f). Kumpikaan riskeistä ei ole itsessään, kertaluontoisena, vakava. Kuitenkin mahdollisesti ongelman toistuessa asiakas saattaa närkästyä jatkuvista viivästyksistä (riskin 1a tapauksessa) ja toisaalta voittoa tavoittelevan yrityksen tulisi pyrkiä maksimoimaan tehokkuutensa (riski 2f). Riskien lykkääminen ja hyväksyminen pyritään siis välttämään. Jäljelle jää lievennysstrategian kehittäminen.

Vaikka tavoitetilanne onkin riskien poistaminen kokonaan, pitää varoa ylireagointia. Voitaisiin hyvin linjata, että jos nämä riskit realisoituvat, aloitetaan tarkempi seuranta. Riskin 2f tapauksessa voidaan määrittää, että esimerkiksi kolmen epäonnistuneen yhteydenottoyrityksen jälkeen neuvotellaan asiakkaan kanssa erikseen mahdollisista vaihtoehdoista, joilla saataisiin aikaan molempia osapuolia tyydyttävä toimintamalli.

Riskin 1a kohdalla strategia onkin todennäköisesti paljon monimutkaisempi. Tietojärjestelmän käyttökatkon syy voi olla joko yrityksen omien laitteistojen pettäminen, tai tietoliikenneoperaattorin yhteysongelma. Agenteqissa on jo valmiiksi olemassa vianselvitysprosesseja esimerkiksi tietoliikenneyhteyksien katkeamisen selvittämiseen. Suurelta osin lievennysstrategioiden suunnittelu onkin olemassa olevien käytäntöjen vakiinnuttamista ja dokumentointia. Riskinhallintastrategiat eivät sovellu tallennettavaksi tietokantaan luettelomaisena rakenteena, vaan riskitietokannan tulisi sisältää ennemminkin vain tieto siitä, mistä ja miten tietyntyyppisten riskien strategiat löytyvät, esimerkiksi wiki-muotoisena.

4.7.8 Riskien valvonta

Edellä on esitetty pieni otos bugi- ja hotfix-prosessin riskinhallinnan käynnistämisestä. OCTAVE Allegro ohjeistaa riskinhallintaprosessin läpikäynnin vain kerran, ja jää yrityksen riskinhallintastrategian linjattavaksi, miten riskinhallintaa pidetään yllä. Riskinhallinnan käyttöönotto on massiivinen kokonaisuus. Jo yhdenkin prosessin läpikäynti, jokaisen osapuolen ja työvaiheen, sekä jokaisen työvaiheen jokaisen uhan osalta vie paljon resursseja yritykseltä. Jos samaa prosessia käsitellään jatkossa esimerkiksi kolmen kuukauden välein, päästään paljon helpommalla, kun raskas perusta

työlle on jo tehty. Kuitenkin on muistettava käydä läpi kaikki vaiheet, eikä tuudittautua turvallisuuden tunteeseen.

Vaikka riskinhallinta otettaisiinkin Agenteqissa käyttöön aluksi vain jossain prosessissa, vaikuttaisi se silti monen työhön. Jokaisen tuotannon työntekijän, joka edes teoriassa on kyseisen prosessin kanssa tekemisissä, tulisi olla tietoinen riskinhallinnan tilanteesta, jotta osaisi tarvittaessa puuttua viiveettä mahdollisiin uusiin riskeihin tai muuttuneisiin olosuhteisiin, ja tuoda ne muiden tietoon.

5 JOHTOPÄÄTÖKSET

5.1 Yhteenveto muodostetusta riskinhallintamenetelmästä

Tämän diplomityön tarkoituksena oli käydä läpi riskinhallinnan teoriaa, ja sen pohjalta löytää helposti lähestyttävä ja käyttöönotettava riskinhallintamenetelmä yritykselle, jolla ei sellaista ole ennestään käytössä. Luvussa 2 käytiin läpi riskinhallinnan perusasioita ja lähtökohtia teorialähteiden pohjalta. Luvussa 3 tuotiin esiin Agenteq Solutions Oy:n toiminnan ominaispiirteitä, joihin uuden riskinhallinnan tulisi mukautua. Lisäksi esiteltiin OCTAVE Allegro -riskinhallintamenetelmä, jota käytetään pohjana luotaessa menetelmää Agenteqin käyttöön.

Pääpiirteittäin riskinhallinta koostuu neljästä vaiheesta: riskien tunnistaminen, riskianalyysi, riskisuunnittelu ja riskinvalvonta. Näiden vaiheiden lisäksi OCTAVE Allegrossa on valmistelevia vaiheita, joissa kartoitetaan resurssit, käydään läpi resurssien riskialttiit kohdat, ja kartoitetaan uhat, jotka voisivat päästä vaikuttamaan resurssiin.

Agenteqin toiminta koostuu erilaisista prosesseista, joista jokainen pitää sisällään toimijoita toimitusketjun eri vaiheista. Prosessien vaiheet ja vaiheiden väliset siirtymät ovat helposti kohdennettavissa tiettyyn osaan toimintaa, kuten esimerkiksi tuotantotiimi tai testaus. Oleellisena osana Agenteqin riskinhallintaa on se, että riskejä on käsittelemässä sellainen ryhmä, jolla on tuntemus kaikkiin prosessin oleellisiin vaiheisiin. Näin saadaan kartoitettua riskejä mahdollisimman kattavasti.

Riskinhallintaprosessi vaatii varsinkin alkuvaiheessa paljon päätöksiä yrityksen johdolta. Kun riskinhallintastrategia, sisältäen tiedon käytettävissä olevista resursseista, ajasta ja yleensäkin riskinhallinnan laajuudesta, on muodostettu, voidaan siirtyä konkreettiseen riskinhallinnan toteuttamiseen. Lisäksi yrityksen johdon linjattavaksi tulevat riskien mittaamiskriteerit ja erilaisten riskien priorisoinnit.

Prosessin alussa käytetään kohdassa 4.2 esitettyä listausta toimijaryhmistä. Nämä poimitaan prosessikohtaisesti, jotta saadaan selville, minkä osa-alueiden henkilöstöä tarvitaan minkäkin prosessin riskinhallintaan. Esimerkiksi projektiprosessiin kuuluvat ryhmät 1, 2 ja 4. Versiopäivitysprosessiin taas kuuluvat ryhmät 1, 3, 5 ja 6.

Seuraavaksi tulee käydä prosessi (tai prosessit, riippuen suoritettavan riskinhallinnan laajuudesta) läpi vaihe vaiheelta, ja konkreettisesti listata joka vaiheessa resurssit, eli käytännössä asiat, joihin uhkia voi kohdistua. Tämän jälkeen resurssikohtaisesti listataan kaikki uhat, jotka voivat niihin kohdistua, ja myös se, miten kyseinen uhka voisi päästä

resurssiin vaikuttamaan. Nämä kaikki tulee listata ylös, ja tallentaa mahdollista myöhempää käyttöä varten.

Kun riskit on saatu selvitettyä, tulee ne käydä läpi prioriteetit huomioiden. Riskeille määritetään toimenpiteet, joilla ne saadaan poistettua tai lievennettyä hyväksyttävälle tasolle. Tämä on erittäin tärkeä osa riskinhallintaprosessia, koska toimenpiteet pitää määrittää siten, että ne ovat käytännössä toteutettavissa, ja kuitenkin samalla mahdollisimman tehokkaita pitkän tähtäimen suunnitelmassa. Myöskin määritetyt resurssit pitäisi ottaa huomioon.

Uhkia, riskejä ja riskistrategioita varten pitää perustaa tietojärjestelmä, jotta ajan myötä saadaan helpommin riskinhallinta osaksi rutiininomaista toimintaa, eikä siten välttämättä tarvitse määrittää strategioita uudelleen ja uudelleen samankaltaisten riskien kohdalla.

5.2 Johtopäätökset

Kuten tässä diplomityössä on useasti painotettu, yrityksen johdolla on erittäin suuri merkitys riskinhallinnan käyttöönotossa ja soveltamisessa. Tarkoituksena olikin tarjota yritykselle ohjeistus riskinhallintaan, ja sitä kautta matala kynnys riskinhallinnan organisoidulle käyttöönotolle toiminnassaan. Diplomityön tuloksena on saatu Agenteqin tarpeet huomioiden vaihe vaiheelta etenevä kokonaisuus, jonka yritys voi ottaa käyttöön.

Menetelmän kuvaus on jätetty varsin abstraktiksi. Tämä johtuu siitä, että Agenteqin tapauksessa riskinhallinnan aloittaminen puhtaalta pöydältä vaatinee niin paljon valmisteluja ja resursseja, että se ei tule kokonaisuudessaan onnistumaan lähitulevaisuudessa. Näinollen esimerkiksi riskitietokannan rakenteeksi ja toimintojen dokumentoimiseksi tulisi aluksi riittämään huomattavasti pienimuotoisempi tapa, jos esimerkiksi riskinhallintaa kohdistetaan aluksi vain tietynlaisiin prosesseihin. Kohdassa 4.7 on annettu esimerkki siitä, miten riskinhallintaprosessi Agenteqissa voisi käytännössä edetä.

Haasteena työssä oli lähdemateriaalin löytämisen vaikeus. Varsinkin kokemuksia OCTAVE Allegro -menetelmän soveltamisesta laajemmin kuin tietoturvariskien hallintaan oli vaikea löytää. Muutenkin Agenteqin toimintatavan eroaminen perinteisistä ohjelmistoprojekteista asetti työlle haasteita. Riskinhallintaa piti käsitellä huomattavasti abstraktimmalla tasolla, ja varsinkin riskinhallintaorganisaation muodostaminen on monimutkaisempaa perinteisen ohjelmistoprojektin vastaavaan verrattuna.

Diplomityön tulosten hyötyjä voidaan kunnolla arvioida vasta tulevaisuudessa, kun riskinhallintaa on otettu käyttöön edes jossain yrityksen toiminnan osa-alueella. Teoriassa mahdollisuudet suureenkin hyötyyn ovat olemassa, kunhan sopivat toimintatavat, yksityiskohdat ja riskinhallintastrategia muotoutuvat.

LÄHTEET

Agenteq Solutions Oy. 2014. Sisäinen viestintä.

Caralli, R. et al. 2007. Introducing OCTAVE Allegro. [WWW]. [Viitattu 28.9.2014] Saatavissa:
http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

Gentile, M. et al. 2006. The Ciso Handbook: A Practical Guide to Securing Your Company. Yhdysvallat, Auerback Publications. 321 s.

Haikala, I & Märijärvi, J. 2004. Ohjelmistotuotanto. Kymmenes, uudistettu painos. Helsinki, Talentum. 440 s.

Keiski, T. 2013. Developing Security in the System Development Lifecycle. Master's Thesis. Turun ammattikorkeakoulu. Business Information Systems. 82 s.

McGhee, P. & McAliney, P. 2007. Painless Project Management: A Step-by-Step Guide for Planning, Executing, and Managing Projects. Yhdysvallat, John Wiley & Sons, Inc. 251 s.

McManus, J. 2004. Risk Management in Software Development Projects. Englanti. Elsevier Butterworth-Heinemann. 172 s.

NIST. 2012. Guide for Conducting Risk Assessment. [WWW]. [Viitattu 28.9.2014]. Saatavissa: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912091

Protiviti Inc. 2013. Effective Positioning of the Risk Management Organization. [WWW]. [Viitattu 30.9.2014]. Saatavissa:
http://www.protiviti.com/en-US/Documents/White-Papers/Industries/
CRO-Series3-Effective-Positioning-Risk-Mgmt-Protiviti.pdf

ScrumGuides. 2014. ScrumGuides.org. [WWW]. [Viitattu 30.9.2014]. Saatavissa: http://www.scrumguides.org/scrum-guide.html

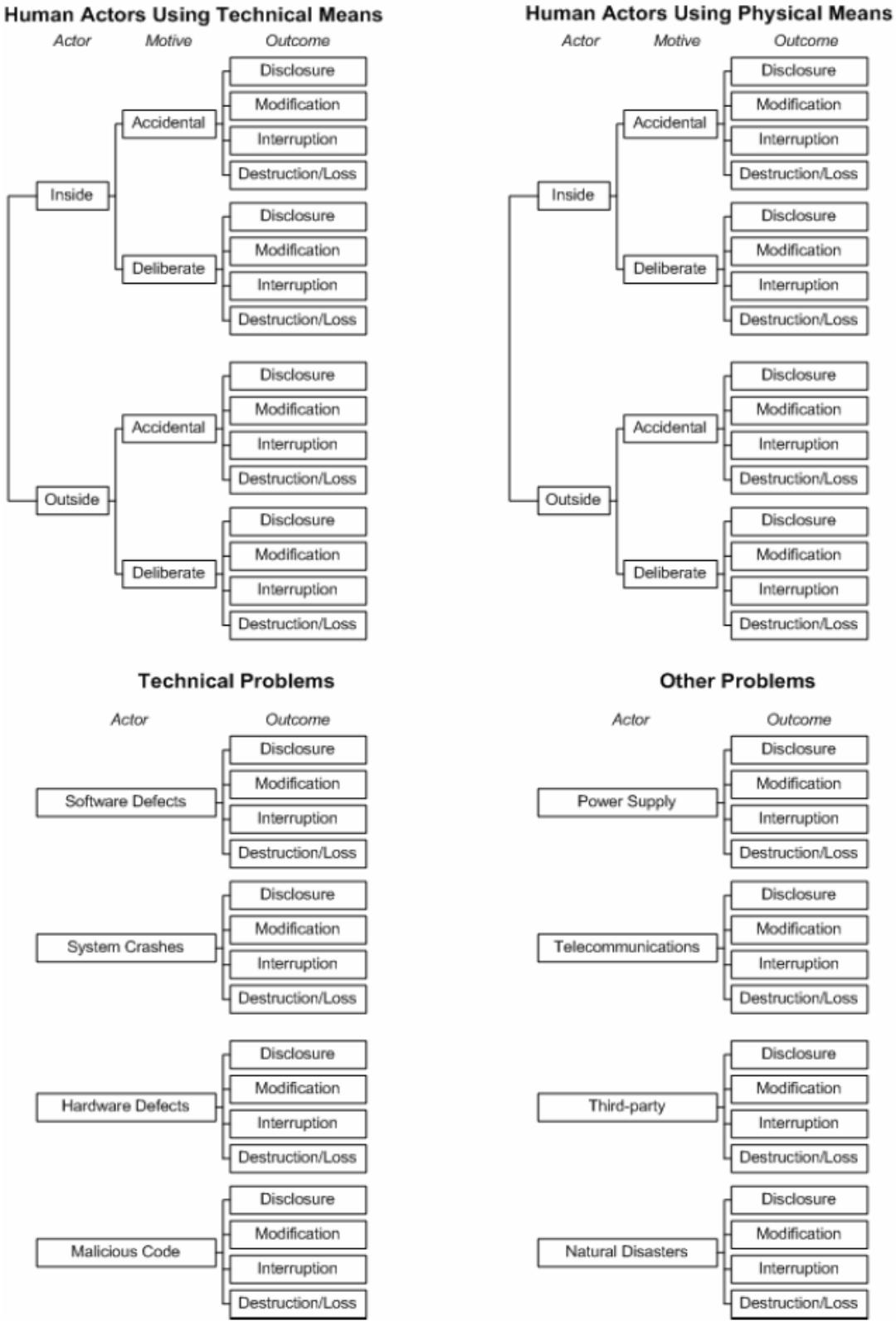
Sommerville, I. 2007. Software Engineering, 8th Edition. Englanti. Addison-Wesley Publishers Ltd. 840 s.

Suomen Riskinhallintayhdistys. Nelikenttäanalyysi – SWOT. [WWW]. [Viitattu 30.9.2014]. Saatavissa: http://www.pk-rh.fi/index.php?page=swot

Talokeskus Yhtiöt Oy. 2014. Tampuuri. [WWW]. [Viitattu 7.10.2014]. Saatavissa: http://www.tampuuri.fi/

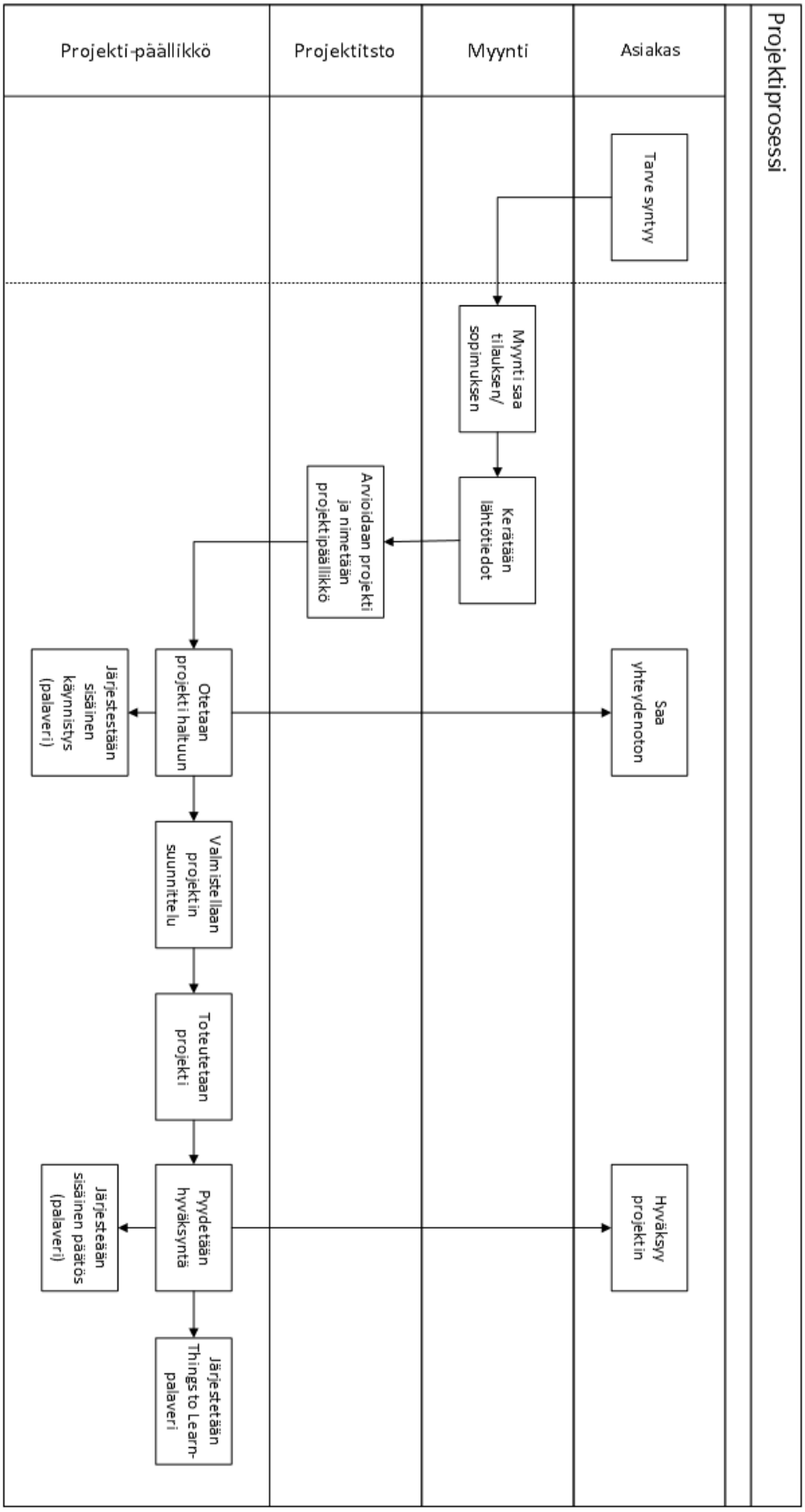
LIITTEET

LIITE 1: OCTAVE Allegron uhkapuut (Threat Tree) avuksi uhkien kartoittamiseen



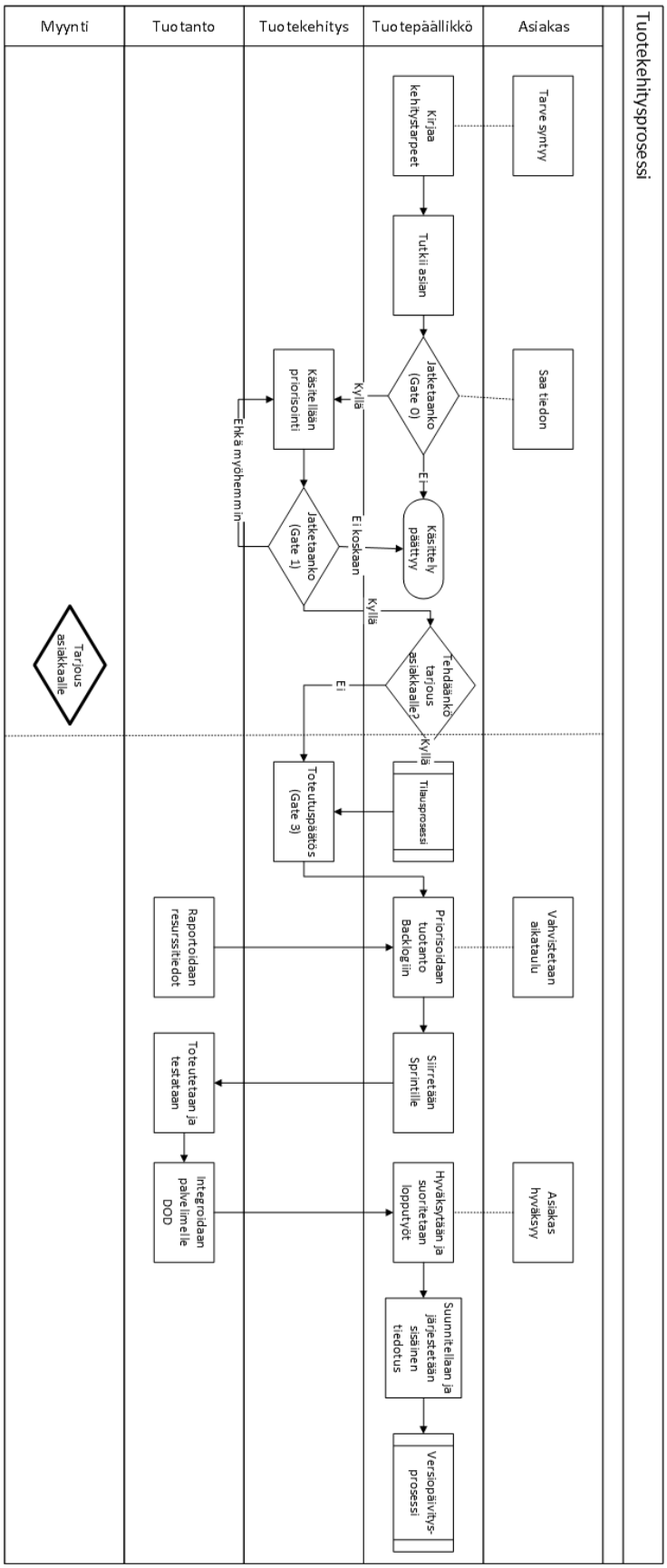
***Kuva 1**: OCTAVE Allegron uhkapuut (Caralli 2007, s. 50)*

LIITE 2: Agenteqin projektiprosessi



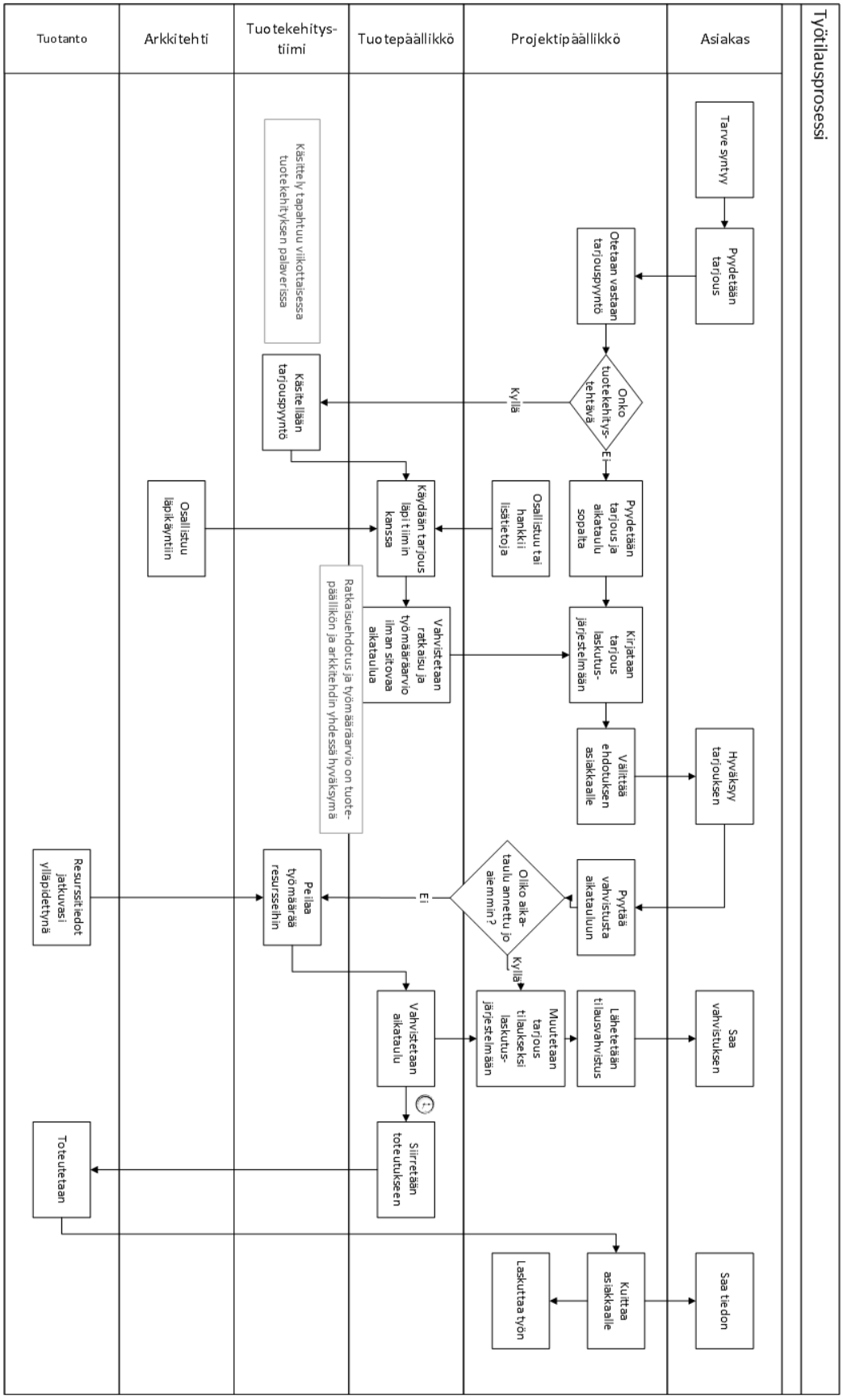
***Kuva 1**: Projektiprosessi (Agenteq 2014)*

LIITE 3: Agenteqin tuotekehitysprosessi



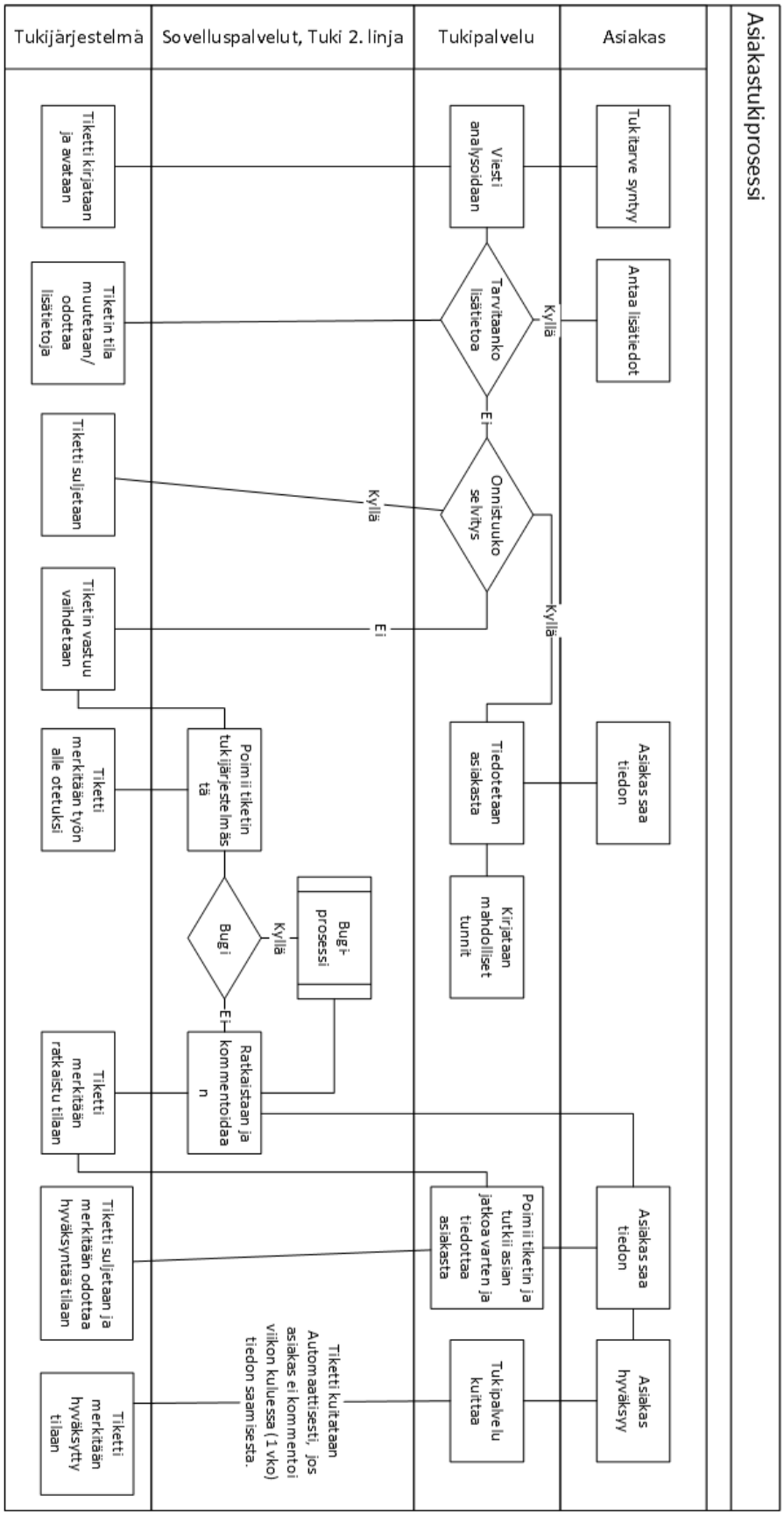
***Kuva 1**: Tuotekehitysprosessi (Agenteq 2014)*

LIITE 4: Agenteqin työtilausprosessi



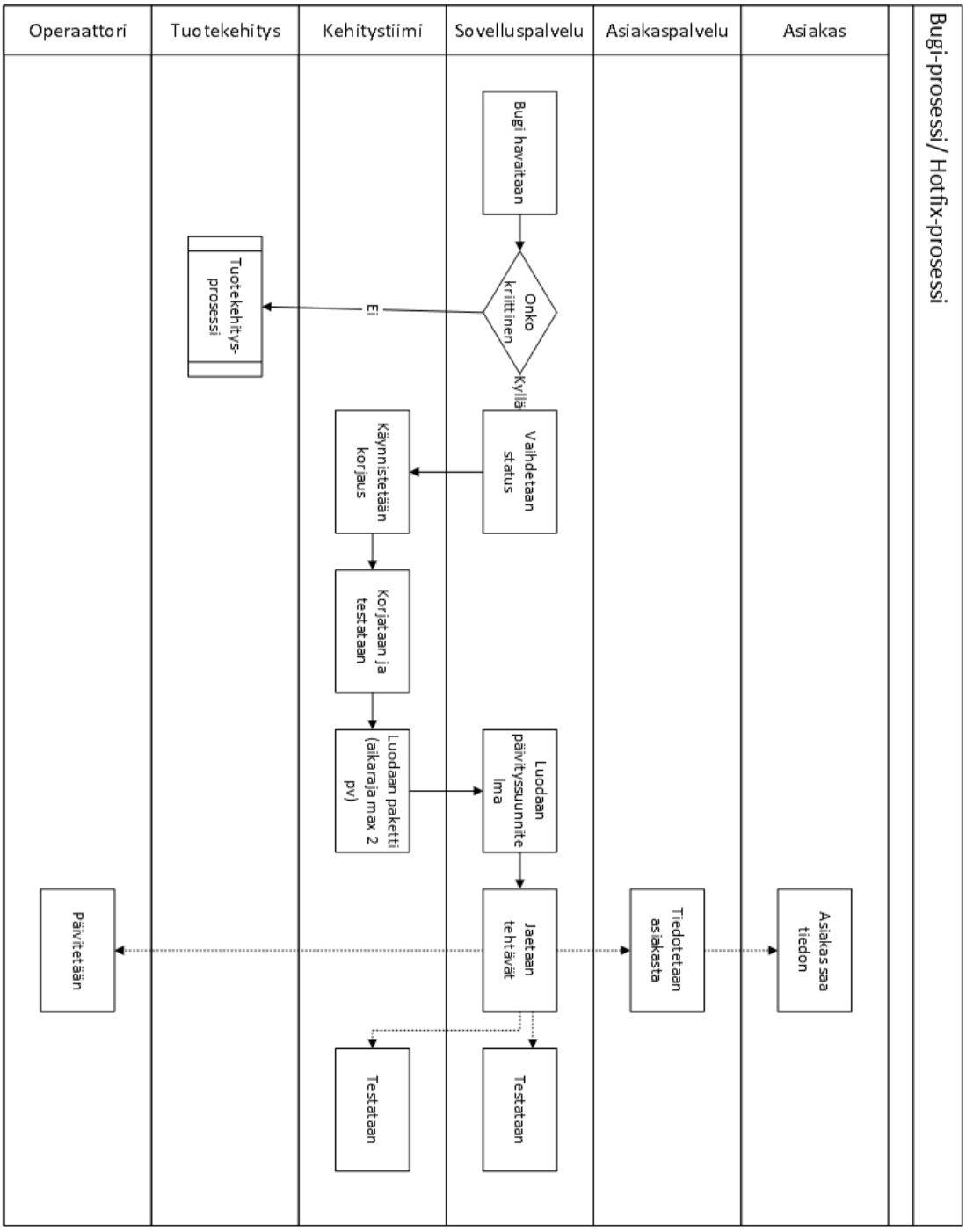
***Kuva 1**: Työtilausprosessi (Agenteq 2014)*

LIITE 5: Agenteqin asiakastukiprosessi



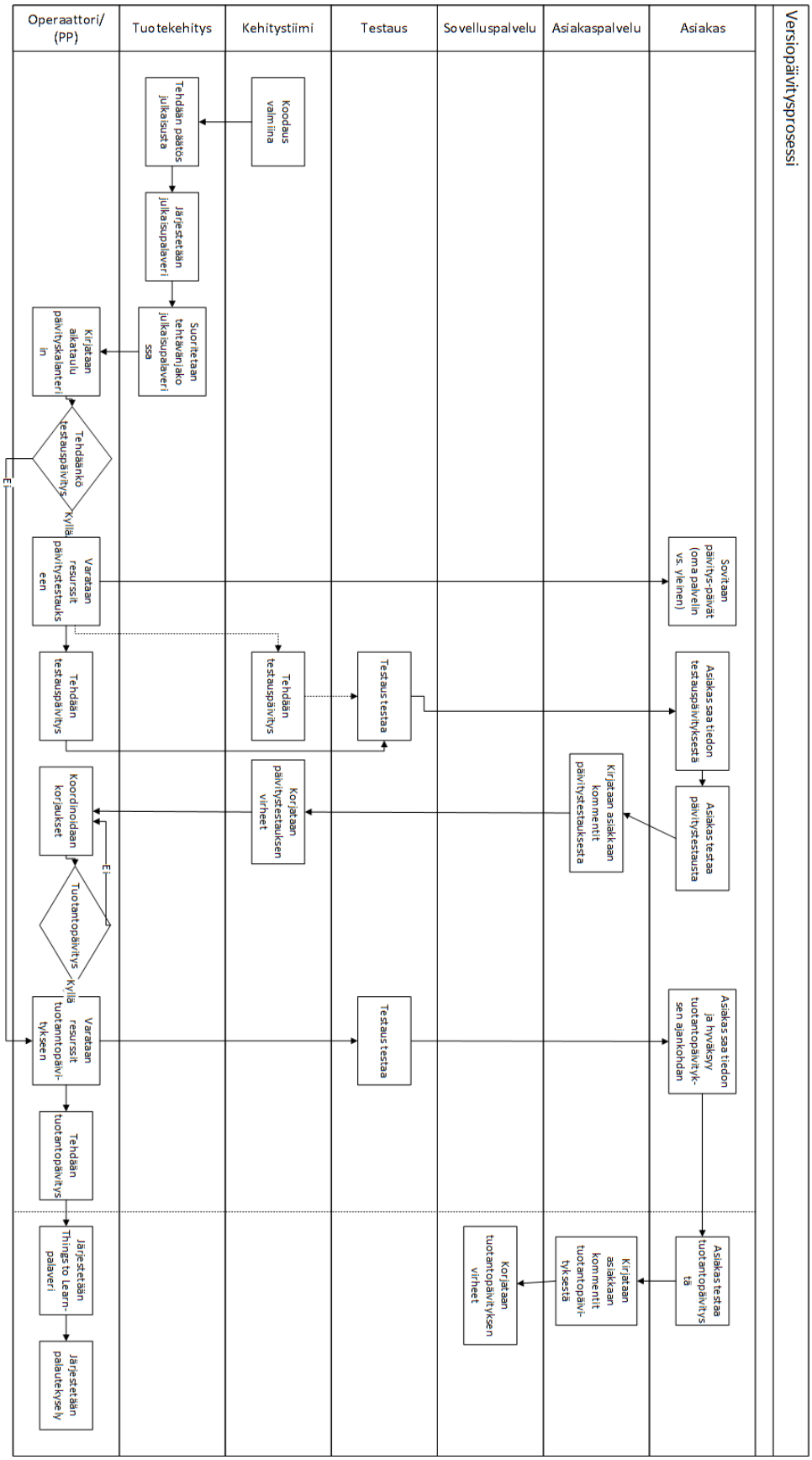
***Kuva 1**: Asiakastukiprosessi (Agenteq 2014)*

LIITE 6: Agenteqin bugiprosessi / hotfix-prosessi



***Kuva 1**: Bugiprosessi / -Hotfix-prosessi (Agenteq 2014)*

LIITE 7: Agenteqin versiopäivitysprosessi



***Kuva 1**: Versiopäivitysprosessi (Agenteq 2014)*